Information Type: --- (Open Distribution/Public Document)
Company Name: NTT DATA Italia
Information Owner: Legal & Compliance

ORGANIZATION, MANAGEMENT, AND CONTROL MODEL OF NTT DATA Italia

Under Legislative Decree 231/2001

General Section

Approved by the Board of Directors on June 25, 2024

ORGANIZATION, MANAGEMENT AND CONTROL MODEL OF NTT DATA ITALIA SPA under Legislative Decree 231/2001

General Section

SUMMARY

DEFINITIONS

Risk areas	The areas of company activity in which, in more concrete terms, the risk of committing the Offences specified in Legislative Decree no. 231/2001 is present
NATIONAL COLLECTIVE NEGOTIATION AGREEMENT	National collective labour agreement applicable to employees of NTT Data Italia S.p.A.
CCNL Executives	National collective labour agreement for managers of companies producing goods and services, currently in force and applied by NTT Data Italia S.p.A.
Code of Ethics and Conduct of NTT DATA EMEAL or Code of Ethics or Code of Conduct	Code approved by NTT DATA EMEAL, modified and adopted by the Board of Directors of NTT DATA Italia including the set of rights, duties and responsibilities that NTT DATA Italia S.p.A. expressly assumes towards its counterparts in the performance of its activities and available on the Company's website and intranet portal
Collaborators	Those who act in the name and/or on behalf of NTT DATA Italia S.p.A. on the basis of a specific mandate or other contractual obligation
Decree	Legislative Decree no. 231 of 8 June 2001 and subsequent amendments and additions
Recipients	Members of the corporate bodies and internal corporate *governance* bodies, employees, collaborators in any capacity, including occasional ones, and all those who have commercial and/or financial relationships of any nature with NTT Data Italia S.p.A., or who act on its behalf on the basis of specific mandates (for example: consultants, suppliers, partners)
Employees	All employees of NTT DATA Italia S.p.A. (including executives).
Relatives	Relatives and in-laws in a straight line up to the second degree (children, parents, grandchildren - such as children of the children - and grandparents, parents in-law and sons-in-law, daughters-in-law, brothers or sisters of the spouse), relatives and in-laws in a collateral line up to the third degree and also cousins (brothers and sisters, grandchild and uncle, as well as cousins); spouse and/or cohabiting partner
Departments	First level organisational structures of NTT DATA Italia S.p.A.
Counterparts	With the exclusion of collaborators, all contractual counterparts of NTT DATA Italia S.p.A., natural or legal persons, such as suppliers, customers and, in general, all persons to or from whom NTT DATA Italia S.p.A. provides or receives any contractual service
Guidelines	The Guidelines for the construction of models of organisation, management and control according to Legislative Decree 231/2001, approved by Confindustria and subsequent amendments and additions
Model 231	Organisation, Management and Control Model under Legislative Decree 231/2001

Model or Organisational model or MOG	Organisation, Management and Control Model under Legislative Decree no. 231/2001 adopted by NTT DATA Italia S.p.A.
NTT DATA Corp.	NTT DATA Corporation
NTT DATE EMEAL	NTT DATA Europe & Latam S.L.U.
NTT DATA Group or NTT DATA Group	NTT DATA Corp. and its subsidiaries
NTT DATA Italia or Company	NTT DATA Italia S.p.A.
Corporate Bodies	The Board of Directors and the Board of Statutory Auditors of NTT DATA Italia S.p.A.
Supervisory Board or Board	Supervisory Board under art. 6, paragraph 1, letter b) of Legislative Decree 231/2001
Public administration	Any Public Administration, including its representatives in their capacity as public officials or persons in charge of a public service, also de facto
Offences or Offence or Offences 231	Relevant offences under Legislative Decree 231/2001
Management hierarchy	The Chairman and Chief Executive Officer of NTT DATA Italia S.p.A.

1 INTRODUCTION

1.1 Adoption of the model under Legislative Decree no. 231/2001 by NTT DATA Italia S.p.A.

Legislative Decree no. 231 of 8 June 2001 (*Rules governing the administrative liability of legal persons, companies and associations, including those without legal personality, in accordance with art. 11 of Law no. 300 of 29 September 2000*) introduced into the Italian legal system - as is now known - a particular system of administrative liability for companies, which applies when the offences listed in the Decree are committed, in the context of the activities carried out by companies.

On January 28, 2006, the Board of Directors of NTT DATA Italia S.p.A. approved the first version of the Organisational, Management and Control Model under Legislative Decree 231/2001 in the knowledge that the implementation of the Model, while representing a choice and not an obligation, allows the Company to have a set of rules, tools and activities suitable to prevent the commission of the offences referred to in the Decree, to hold the Company harmless from the liability stipulated in it in the event that one of the above-mentioned offences is committed, as well as to strengthen its culture of *governance* and raise employee awareness on issues of control of business processes, to stimulate an "active" prevention of the Offences and - more generally - of any illegal conduct within the Company.Following the regulatory changes that have affected the Decree since that date, as well as the development of case law regarding the issue of the companies' administrative liability, over time the Board of Directors of NTT DATA Italia has approved numerous updates and amendments to the Model, also harmonizing and updating the Code of Ethics approved by NTT DATA EMEAL and adopted by the Company.

This document therefore reflects the Model in the version most recently approved by the Company's Board of Directors on June 25, 2024, which follows those approved on June 29, 2023, September 20, 2011, July 29, 2014, November 30, 2016, December 10, 2018 and June 29, 2020.

1.2 NTT DATA Italia S.p.A.

Since 2011 NTT DATA Italia is part of the NTT DATA Corp. Group, based in Tokyo, an international player that provides innovative and quality IT services, products and solutions for customers worldwide, operating in various and different sectors of activity (telecommunications, banking and financial services, insurance, P.A., industry and distribution, utilities, publishing and mass media).

NTT DATA Italia is subject to the direction and coordination of NTT DATA EMEA Ltd. based in London.

1.3 The NTT DATA Italia Model

The Model adopted by the Company is an act issued by the *"executive body"* under art. 6, par. 1, letter a) of Legislative Decree 231/2001, a body that within NTT DATA Italia can be identified with the Board of Directors, which is therefore responsible for any subsequent amendments and additions to the MOG. The Chief Executive Officer of the Company has the right to make changes and additions to the text of the Model that are only of a formal nature.

The basic principles described in the General Part of the Model apply to NTT DATA Italia and are shared by the subsidiaries; they must be complied with in all company activities carried out both in Italy and abroad. The organisational, management and control models of the subsidiaries are in fact inspired by the same values and general principles described below.

The adoption of the Model is not only necessary to make the Company fully compliant with Decree 231/2001, but is also essential to raise awareness among all those who work for the Company to a transparent behaviour, dictated by full compliance with the law, as already highlighted in the introduction above. The purpose is to build and maintain a structured and organic system of procedures and control activities, aimed at preventing the commission of the various types of offences covered by Decree 231/01.

This document is addressed to all those who work for the achievement of the purpose and objectives of NTT DATA Italia, in particular, as specified in the previous "Definitions": the members of the Company's corporate bodies and governance bodies, employees, external consultants, suppliers, customers and, in general, all third parties with whom NTT DATA Italia has relationships regarding its corporate activities. In this context, the Model was drawn up in compliance not only with the dictates of the Decree, but also with the guidelines developed by trade associations, in particular the indications of Confindustria with the document *"Guidelines for the establishment of organisation, management and control models"* issued on 7 March 2002 (most recently updated in 2021).

This document has been prepared with the aim of supporting the understanding of the Company's organisational, management and control system through a reference context that also highlights where the most up-to-date information on the choices and instruments in place can be found. For this reason, it often contains references to other company documents.

As a subsidiary of the parent company NTT DATA Corp., NTT DATA Italia is required to implement the J-SOX regulation (Japan's Financial Instruments and Exchange Law), which requires all companies listed on the Japanese stock exchange and its subsidiaries to strengthen their internal governance in order to ensure accurate and complete disclosure of financial information. Within the NTT DATA Group, specific internal auditing activities are therefore carried out in accordance with the above-mentioned regulations.

1.4 General principles of the Model

The Model adopted by NTT DATA Italia is based on the following general principles:

a) **Knowledge of the risks through** the mapping of the Company's "sensitive processes" and the evaluation of the level of risk, also in light of the reasons set out in the Position Paper issued by the Italian Association of Internal Auditors;

b) **Definition of values and rules of conduct,** collected in the Code of Conduct and in company procedures, manuals and information technology, with particular attention to those regarding the financial management;

c) **Clear assignment of roles and powers,** through an organisational structure, a system of simple and transparent powers and delegations, with the indication, when required, of the thresholds for approval of expenses;

d) **Sharing of governance and management rules,** as described in the statutes of the corporate bodies, aimed at ensuring an adequate level of collegiality in the decision-making process;

(e) **Implementation of an effective internal control system,** based on the following rules:

- Each operation, transaction and action must be: verifiable, consistent and appropriate, and adequately supported at document level so that checks can be carried out at any time to certify the characteristics and reasons for the operation and identify who authorised, recorded and verified the operation;
- No one should be able to manage an entire process autonomously, i.e. the principle of the separation of functions and powers must be complied with;
- Authorisation powers must be assigned in a manner consistent with the assigned responsibilities;
- The control system must document the performance of the controls, including supervision;

f) **Surveillance activities on the effectiveness** of the control system and, more generally, on the entire Organisation, management and control model:

- The assignment of the task of promoting the effective and correct implementation of the Model to an internal Supervisory Board within the Company, also through the monitoring of company behaviour and the right to constant information on activities relevant for the purposes of Legislative Decree 231/2001;
- The provision of adequate resources to the Board so that it is supported in the tasks entrusted to it to achieve the results reasonably achievable;
- The activity of verifying the functioning of the Model with consequent periodic updating (ex post control);
- Awareness raising and dissemination of the established rules of conduct and procedures at all company levels;

g) Transparent and widespread communication of values, principles and rules, accompanied, where necessary, by specific training activities on the instruments that make up the Model and that the Company implements to prevent all unlawful conduct;

h) Application of disciplinary mechanisms and sanctions for conduct not in line with the application of the Model by NTT DATA Italia.

This Model is also consistent with the key principles indicated by the NTT DATA Corp parent company, but it also contains specific features inherent in the organisational structures and business activities of NTT DATA Italia, with further specific measures related to the specific nature of its business and with close coordination with the procedures and protocols of the Quality Management System and with the relevant ISO 9001 Certification which the Company holds.

2 RISK MAPPING

2.1 Introduction

The Company's organisational model is implemented taking into account its effective compatibility with the current company organisation, so as to integrate it efficiently with the business operations and, if necessary, undergo the necessary changes in a flexible manner.

For this reason, the Supervisory Board, which will be discussed in detail below, has the powers necessary for the purposes of monitoring and verifying the Model.

As suggested by the Confindustria Guidelines, the creation and implementation of a Risk Management System includes the following elements and steps:

1. *identification and analysis of risks and protocols;*
2. *identification of the components necessary for the system:*
3. *regulation and appointment of the Supervisory Board;*
4. *definition of the Company's Code of Ethics;*
5. *definition of the specific sanctions system.*

2.2 Risk identification and protocols

For the purposes of preparing the Model, first of all, over time NTT DATA Italia has identified and updated the conduct at risk with respect to the company functions and the offences stipulated by Legislative Decree. 231/2001, connected to them. Following this analysis and study phase, the Model aims:

1) To make all those who work in the name and on behalf of NTT DATA Italia in the areas of activity at risk aware that, in the event of violation of the provisions contained in it, they may commit an offence punishable by criminal and administrative sanctions, not only against themselves, but also against the company;

2) Reiterate that these forms of unlawful conduct are strongly condemned by the Company because (even if the Company were in a position to take advantage of them) they are in any case contrary to the provisions of the law in force and to the principles affirmed by the Company policies and by the Code of Conduct and that the Company undertakes in the most determined way to prevent such conduct;

3) By means of monitoring the activities at risk, to allow the Company to intervene promptly to prevent and counteract, as far as possible, the commission of the offences themselves, namely:

a. identifying the activities in which offences may be committed, thus periodically mapping and updating the company areas in which the activities most at risk are carried out;
b. providing specific protocols aimed at planning the formation and implementation of the Company's decisions in relation to the Offences to be prevented;
c. identifying methods for managing financial resources that are suitable for preventing the commission of the Offences;
d. Stipulating the obligations to provide information to the body responsible for supervising the operation of and compliance with the models;
e. introducing information and awareness systems at all company levels regarding the established rules of conduct and procedures and an effective disciplinary system capable of sanctioning non-compliance with the measures indicated herein;

f. in relation to the nature and size of the organisation, as well as the type of activity carried out, stipulating appropriate measures to ensure that the activity is carried out in compliance with the law and to promptly detect and eliminate situations of risk.

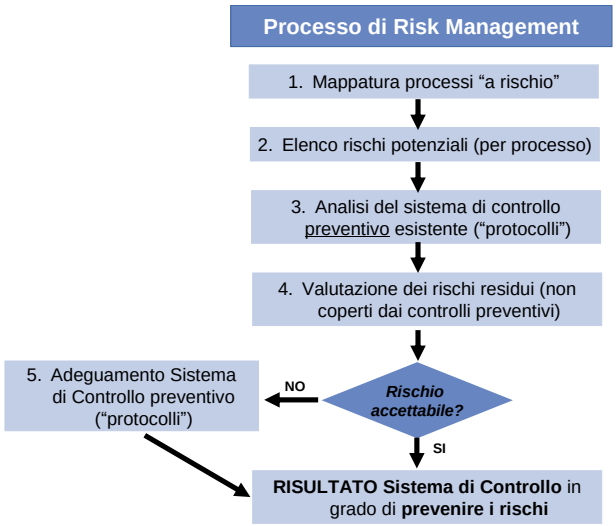
As stipulated in Article 6(1)(b) and (c) of Regulation (EC) No 880/2004, the Commission shall, in accordance with the procedure stipulated in Article 6(2), adopt the measures necessary to comply with the provisions of Regulation (EC) No 880/2004. 2, of Legislative Decree 231/2001, the implementation of the *risk management* system of NTT DATA Italia is divided into two phases:

a) the identification of risks through the analysis of the company context to highlight where (in which area/sector of activity) and according to which methods hypothetical offences may occur;

b) evaluation of the control system, i.e. verification that the existing system within the Company is adequate to maintain the highlighted risks at an acceptable level and that any modification/improvement is planned and implemented, with the objective of reducing the minimum threshold of the acceptable level of the identified risks.

From a conceptual point of view, reducing a risk involves intervening (jointly or severally) on two determining factors:

- the probability of the event happening;
- the impact of the event itself.



The identification of company areas/types of behaviour at risk is assessed on the basis of the principle of potential occurrence both in relation to the business activity and with respect to the involved departments.

This assessment, although of a preventive nature, is the starting point for the qualitative definition of risk as "*acceptable*" by the Company, since the incidence and probability of occurrence of the specific risk have been linked.

However, in order to operate effectively, the system cannot be reduced to an occasionalactivity, but must be translated into a continuous (or periodic) process, to be repeated with particular attention in times of corporate change (for example: opening of new offices, expansion of activities, acquisitions, reorganizations, etc.).

2.2.1 The definition of *"acceptable risk"*

The conceptual threshold of risk acceptability is represented by a system of prevention that cannot be circumvented unless done so intentionally.

With regard to corporate offences, for example, the process of preparing the annual accounts, the management of *price sensitive* information and the procedures for the functioning of corporate bodies have been verified.

In addition to the objective aspect or the area of possible violation, due consideration was also given to the subjective perspective, i.e. who are the people, active or passive, involved in any violations.

In the context of this process of reviewing processes/functions at risk, it is advisable to identify the persons affected by the monitoring activity, which in certain particular and exceptional circumstances, could also include those who are linked to the company by mere relationships of para-subordination, such as for example external consultants, or other collaborative relationships, such as business partners, as well as employees and collaborators of the latter.

In the same context, it is also advisable to carry out *due diligence* whenever "indicators of suspicion" (e.g. conducting negotiations in areas with a high rate of corruption, particularly complex procedures, presence of new personnel unknown to the Company) have been identified during the risk assessment process relating to a particular commercial transaction.

The processes in the financial area are clearly important for the purposes of the application of Legislative Decree 231/2001, and it is probably for this reason that it deals with them separately (art. 6, par. 2, letter c), even though a careful analysis of the evaluation of the business areas "at risk" should, however, identify the financial one as having clear importance.

2.2.2 Analysis of potential risks

The analysis of potential risks has been linked to possible subjective behaviour that may lead to the commission of Offences for each involved company area.

The summary of this analysis is represented by a survey form (*check list* included in the special section of the Model) in which the Company's corporate functions and the specific activities of persons and corporate bodies were compared to the possible offences relevant to NTT DATA Italia.

2.2.3 Evaluation/construction/adjustment of the preventive control system

The activities described above are completed with a prior evaluation of the existing control system, in order to allow the Supervisory Board to analyse the deviations between the latter and the prevention Model, and to adapt it when necessary.

The system of preventive checks aims to ensure that the risks of commission of the Offences, as identified and documented in the previous phase, are reduced to an "acceptable level", as defined above.

It is, in essence, a matter of implementing what Legislative Decree 231/2001 defines as *"specific protocols aimed at planning the formation and implementation of the company decisions in relation to the offences to be prevented"*, an activity that NTT DATA Italia has implemented through the adoption of instruments, control systems, procedures and

company policies in line with the above-mentioned regulatory instructions.

2.3 Risk detection and mapping

NTT DATA Italia has carried out and periodically updates the analysis of company processes and operations in order to identify the areas at risk (risk mapping), meaning by the latter the areas of activity that are affected by potential offence cases under Legislative Decree no. 231/2001.

In this sense, the identified risks were identified and mapped with specific reference to the company activities actually carried out and the functions actually performed by the operators.

This analysis has shown which activities are most exposed to the commission of the offences indicated in the Decree or in any case to be monitored. These Offences and the macro-areas of activity thus identified were the following.

2.3.1 Penalties against the Public Administration (Artt. 24 and 25, of Legislative Decree 231/2001)

The activities considered sensitive in relation to Offences against the Public Administration are:

a) Negotiation/signing and/or performance of contracts/conventions of concessions with public entities, which are reached through negotiated procedures (direct award or private negotiation);

b) Negotiation/signing and/or performance of contracts/conventions of concessions with public entities which are reached through public procedures (open or restricted);

c) Negotiation/signing or performance of contracts with public entities that are reached through private negotiations;

d) Negotiation/signing and/or performance of contracts with public entities that are reached through open or restricted procedures;

e) Management of relations with bodies/supervisory authorities relating to the performance of activities regulated by law;

f) Management of acquisition activities or management of contributions, subsidies, financing, insurance or guarantees granted by public bodies;

g) Request for occasional/ad hoc administrative measures necessary to carry out activities instrumental to typical company activities;

h) Preparation of tax returns or substitutes for tax or other declarations for the settlement of taxes in general;

i) Compliance with public bodies, such as communications, declarations, filing of deeds and documents, files, etc., different from those described in the previous points and in the sanction checks/assessments/procedures resulting from them;

j) Activities that involve the installation, maintenance, updating or management of software by public entities or provided by third parties on behalf of public entities;

k) Other *"sensitive activities"*: relations with the institutions and administrations of the State.

2.3.2 Corporate Offences (art. 25-*ter*, of Legislative Decree 231/2001)

The sensitive activities in terms of corporate offenses are the following:

a) Preparation of the annual accounts and periodic interim reports;

b) Relations with shareholders, audit firm, board of statutory auditors, audits and relations with supervisory authorities;

c) Capital transactions and allocation of profit;

d) Communication, carrying out and minutes recording of Shareholders' Meetings;

e) Management of business relations and negotiations with private customers and suppliers (with reference to the offence of bribery between private individuals and incitement to corruption between private individuals).

2.3.3 Offenses against health and safety in the workplace (art. 25-*septies*, of Legislative Decree 231/2001)

The activities considered sensitive in relation to health and safety offences at work, are:

a) Establishment and control of the management system of health and safety in the workplace;

b) Performance phases of procurement, works and supply contracts;

c) As a client entrusting works and/or services within its own facilities.

2.3.4 Computerized offenses (art. 24-*bis*, of Legislative Decree 231/2001)

The activities and behaviour that represent the types of computer offences are:

a) Access to a computer system protected by security measures;

b) Managing codes, keywords, credentials to access computer systems protected by security measures;

c) Reproducing, disseminating, duplicating, selling or making available to third parties proprietary computer programs or other intellectual property in violation of copyright protection rules.

2.3.5 Offences relating to the violation of copyright (art. 25-*novies*, Legislative decree 231/01)

The activities that constitute offences in the field of copyright are:

a) Duplicating, importing, distributing, selling, leasing, disseminating/transmitting to the public, holding for commercial purposes, or otherwise for profit, without having the right, proprietary computer programs, protected databases or any work protected by copyright or related rights, including works with literary, musical, multimedia, cinematographic or artistic content;

b) Disseminating an intellectual work or part of it by telematic means without having the right to do so;

c) Implementing file sharing practices;

d) Sharing any file through peer-to-peer platforms.

2.3.6 Inducement to not make statements or to make false statements to the judicial authorities (art. 25-*decies,* Legislative decree 231/01)

The activities that can be traced back to the Offence in question are:

a) Providing instructions to influence a person required to make statements before the Judicial Authority in order to obtain favourable treatment from the latter in relation to ongoing proceedings or investigations.

2.3.7 Employment of third party citizens whose stay is illegal (art. 25-*duodecies*, Legislative decree 231/01)

The activities considered sensitive in relation to the Offence in question are:

a) Selection and recruitment of personnel;

b) Management of non-EU employees.

2.3.8 Receiving, laundering and using money, goods or benefits of illicit origin (art. 25-*octies,* Legislative Decree 231/2001)

Although the risk of commission of the above Offences appears to be entirely theoretical and residual, taking into account the sectors of activity in which NTT DATA Italia operates, it was considered useful to dedicate, in the Special Section of the Model, a specific paragraph to this type of Offences in view of their significant social danger, indicating measures, procedures and control instruments - for the most part already present within the NTT DATA Italia structures - suitable for preventing the relative risk of commission.

2.3.9 Self-money laundering (Article 25-*octies,* Legislative Decree 231/2001)

Article 3, paragraph 5, of Law no. 186 of 15/12/2014 ("*Provisions on the emergence and return of capital held abroad as well as for the strengthening of the fight against tax evasion.Provisions on self-laundering*") has amended Article 25 -*octies* of Legislative Decree231/2001, introducing in the category of possible offences, the offence of self laundering under Article 648-ter.1 of the Criminal Code, punishable from 1 January 2015.This offence, the sensitive company activities and the related controls, will be dealt with in a specific paragraph in the Special Section of the Model, taking into account both the complexity involved in identifying the company areas in which it could theoretically be committed, and the lack, at present, of consolidated jurisprudential guidelines on the subject (the introduction of self-laundering in our legal system, as well as in the "catalogue" of 231 Offences, took place recently - as mentioned above).

2.3.10 Offences relating to non-cash payment instruments and fraudulent transfer of values (art. 25-*octies*.1, Legislative Decree 231/2001)

The activity considered sensitive in relation to the offences in question is the processing and diffusion of computer instruments and programs, as well as the fictitious attribution of ownership of companies, company shares or stocks or of corporate offices in order to circumvent the provisions on anti-mafia documentation in connection with the award or execution of contracts or concessions.

2.3.11 Crimes against individuals (Article 25-*quinquies,* Legislative Decree 231/2001)

On November 4, 2016, Law no. 199 of October 29, 2016 entered into force, inserting into Article 25-quinquies of Legislative Decree 231/2001 the new offence of "illicit brokering and exploitation of labour" (Article 603-bis of the Italian Criminal Code), the so-called "*illegal job brokerage*" which punishes the recruitment and hiring of manpower for the purpose of exploiting them for work.
The activities considered sensitive in relation to the crime of "illegal job brokerage" are those relating to the management of personnel used in subcontracting.

2.3.12 Tax offences (Article 25-quinquiesdecies, Legislative Decree 231/2001)

The activities considered sensitive in relation to tax offences are:

a) Active billing and debt collection activities;

b) Passive billing activities and suppliers' payment;

c) Suppliers selection and management;

d) Cash and current account management;

e) Compliance with tax and social security obligations;

f) Storage of accounting records;

g) Payment of taxes;

h) Management of relationships with Public Officials in case of audits/inspections.

2.3.13 Contraband offences (art. 25-s*exiesdecies*, Legislative Decree 231/2001)

The activities considered sensitive in relation to the offences in question are:

a) Fulfilment of border rights;

b) Selection and management of suppliers.

2.3.14 Other activities subject to control

In addition to the controls and monitoring directly concerning the areas and activities within which the above mentioned Offences may theoretically be committed, Model 231 provides further, specific controls for the following processes of "supplies" or instruments management:

a) Financial transactions;

b) Procurement of goods and services;

c) Use of material resources with environmental impact;

d) Consulting and professional services;

e) Utility concessions (donations, scholarships, sponsorship of events);

f) Administrative, financial and accounting management necessary for the company's management;

g) Human resources management (selection and recruitment of personnel, incentive system).

Among the areas of activity at risk, the Model has in fact considered not only those having a direct relevance as activities that could theoretically invite criminal conduct, but also those having an indirect and instrumental relevance in the commission of the Offences. In particular, instrumental activities are those in which the factual conditions that make it possible to commit Offences within the areas and activities specifically considered at risk of crime in the Model are present.

3 VALUES AND RULES OF CONDUCT

3.1 Code of Ethics and Conduct of NTT DATA EMEAL

NTT DATA EMEAL has collected and described the values common to all those who operate within the NTT DATA Group in the Code of Ethics and Conduct of NTT DATA EMEAL, approved and updated periodically by the competent management body.

This Code expresses the ethical commitments and responsibilities in the conduct of business and corporate activities undertaken by NTT DATA Italia towards all stakeholders, in the belief that ethics can be pursued in conjunction with corporate success.

The document is available on the **NTT DATA Italia website** and on **the company's intranet**, and is available in Italian and English (editions are also available in other languages).

3.2 Policies, procedures and instructions

Policies, procedures and instructions describing sensitive processes and standard behaviours have been developed and disseminated in order to provide NTT DATA Italia employees and collaborators with guidance on the behaviours that the Company considers to be in line with the values expressed in the Code of Conduct and in this Model.

All company policies and procedures are sent/communicated to the individual employees whenever there are updates of content or form, and usually published on the company intranet.

3.3 Procedures on the management of financial resources

The Company's financial transactions are documented and reported in processes that clearly and transparently codify the activities, indicating the responsible authors according to the corporate organisation.

Monetary accounting entries are made in accordance with current accounting standards and NTT DATA Italia ensures the use of homogeneous methods and practices among the various units responsible for preparing its own administrative-accounting reports and that of its subsidiaries.

4 ORGANISATIONAL SYSTEM, ROLES AND POWERS

4.1 Characteristics of the organisational Structure

NTT DATA Italia is equipped with organisational tools based on the general principles of:

- Awareness within the Company and the Group;
- Indication of roles (including assigned powers);
- Indication of reporting lines.

4.2 Definition of roles

The definition of roles is such as to ensure that a process is never followed independently by a single person, both in the case of operational processes of project development and management, and in the case of internal support processes.

The operational processes of project development and management, which, in other words, represent the sales and production processes, are overseen by the lines through work teams composed of different qualifications, where each contributes to the formulation of proposals and solutions to the customer, according to a collaborative style and based on their skills and qualifications. During the project development and management phases, operations that have an impact, even if only potential, on the company's financial resources (both incoming and outgoing) are monitored and documented. Control is the responsibility of persons in charge of the monthly Business Reviews and of the Management, through the reports produced by the Administration, Finance and Control Departments - *AFC* (even if only "**Finance**") which, among other things, is responsible for reporting conduct not in line with the standards.

The AFC Department, on the one hand, supports the operational guidelines regarding the generation and use of financial resources related to the characteristic management, on the other hand it supports the top management in the management of financial resources related to assets, extraordinary and tax management. The management and the corporate bodies are responsible for monitoring the economic and financial performance of operations on the basis of the reports prepared by the AFC Function.

Advances in qualifications within the operational lines and changes in the role of personnel in general are

communicated to employees of the Company (and of the Group, if they take place within Corporate Departments).

4.3 System of proxies and powers of attorney

The system of proxies and powers of attorney ensures the functioning of the company by reducing the powers required by the Board of Directors, the Chief Executive Officer and the various proxies.

"*Proxy*" means the internal act of assigning tasks and functions through organisational communications and company procedures; "power of *attorney*" means the unilateral legal transaction whereby the company assigns powers of external representation to third parties. Holders of a position requiring powers of representation shall be granted a power of attorney that is appropriate and consistent with the assigned tasks.

The main features of the proxy system are as follows:

- The proxy reflects the organisational position of the person receiving it, combining management power and relevant responsibility;
- Each power of attorney clearly and unambiguously expresses the powers and the empowered person.

The distinctive elements of the power of attorney system are:

- The power of attorney is granted exclusively to persons with delegated powers by means of specific acts that describe the powers of representation and, where necessary, the spending powers as well as compliance with the Company's Organisational Models and Code of Ethics;
- High value purchases (thresholds indicated in the powers of attorney) must be authorised by the CEO;
- Purchase orders must be issued by the Purchasing Manager (also verified by Management Control) and their traceability is guaranteed through the use of specific information technologies (e.g. Supplier Portal).

5 CORPORATE GOVERNANCE AND CORPORATE MANAGEMENT

5.1 Corporate Governance Model

In conjunction with the request for listing on regulated markets (first half of 2006), the Company began a process of adapting its Corporate Governance Model to the requirements of the Code of Conduct for Listed Companies with the aim of guaranteeing its shareholders an effective and transparent system of governance and management.

The Corporate Governance Model was subsequently adapted and simplified following the decision to postpone the listing on the Stock Exchange.

Currently, also following the recent changes in the corporate and control structure, the Corporate Governance Model is summarised in the Board of Directors, as well as in the Board of Statutory Auditors.

5.2 Corporate Committees

The Company and Group Committees are operational. For example, the Management Committee is active and deals with strategic issues for the development of the Group in the Business Rewiew, in which commercial priorities are defined and the annual budget is drawn up, and the economic performance is presented in the light of the company's objectives.

6 INTERNAL CONTROL SYSTEM

6.1 The Administration, Finance and Control Department

Within the NTT DATA Italia company organisation, the departments responsible for the functioning of the internal control system have been identified in order to group them under the title of "Administration, Finance and Control Department, as already mentioned in the previous paragraph 4.2.. Those who manage and control the Company's financial resources act according to the same principles and the same rules of conduct, adopting a single control Model based on similar processes, tools and operating techniques except for specific business activities or country characteristics.
The head of the Department is the Chief Financial Officer/CFO, who defines the organisational structure of the units for which he is responsible, and organises the planning and control processes, in accordance with procedures and timescales aligned with the rules and requirements for guidance and supervision expressed by the Top Management and the Corporate Bodies.

6.2 Processes and tools

The internal control system is defined as the set of processes implemented by the *management* to provide reasonable assurance of the achievement of management and *compliance* objectives, such as the effectiveness and efficiency of operating activities, the reliability of company, accounting and management information, both for internal purposes and for third parties, and absolute compliance with the company and group laws, regulations, rules and policies.

7 SUPERVISORY BOARD

7.1 Appointment and structure of the Board

The Board is a collective body made up of three standing members, one of whom acts as Chairman, chosen by the majority of the Board, where not already indicated by the Board at the time of appointment. The collective body has the following structure:

- An external professional with expertise in legal, management, analysis of control systems or, in any case, with a high level of experience in issues specifically related to the activities of the Supervisory Board[1];
- An internal member belonging to the NTT DATA Group.

The Board of Directors, reporting to the Shareholders' Meeting, has the power to appoint and revoke the members of the Board - on valid grounds, also related to organisational restructuring of the Company. The members of the Board are chosen from qualified individuals and experts in the above-mentioned fields, with an adequate degree of

[1] Provision updated by Board resolution of June 29, 2023.

professionalism and meeting the requirements of independence, autonomy and honourable character, also from the point of view of the absence of criminal convictions, as better indicated below. The members of the Board may be appointed either from external parties or from within the Company. The members of the Board are not subject, in this capacity and within the scope of the performance of their duties, to the hierarchical and disciplinary power of any corporate body or department.

The Supervisory Board's term of office is usually three years, but the Board can establish a shorter term of office. At the end of the three-year period - or the shorter period established by the Board -, the Supervisory Board continues to perform its functions as an extension until the appointment of new members by the Board of Directors. The members of the Supervisory Board are eligible for re-election.

The internal members of the Board are removed from office in the event of voluntary termination of employment or collaboration with NTT DATA and dismissal for just cause. In the event of the resignation, withdrawal, incapacity, death, revocation or forfeiture of a member of the Board, the Board of Directors will immediately replace him/her. The Chairman, or the most senior member, is required to promptly notify the Board of Directors of the occurrence of one of the cases which make it necessary to appoint a new member of the Board.

In the event of resignation, withdrawal, incapacity, death, revocation or removal of the Chairman, the latter is replaced by the oldest member, who remains in this position until the date on which the Board of Directors has resolved to appoint a new Chairman of the Board.

For all other aspects, the Supervisory Board operates in accordance with the provisions of its Regulations, as follows. The Supervisory Board regulates its supervisory and control activities by means of a set of Regulations to be submitted to the Board of Directors of the Company for relevant acknowledgement at the first useful meeting, as well as any amendments that the Board deems necessary to make to it during its mandate.

7.2 Jurisdiction and grounds for (in)eligibility, revocation and suspension

Competences

The responsibilities of the members of the Supervisory Board, roughly divided between legal and organisational responsibilities, can be summarised as follows:

Legal competences: i.e. in-depth knowledge of the methodologies used to interpret the laws with specific preparation in the analysis of the types of crimes and in the identification of possible sanctionable conduct.
Such preparation presupposes familiarity with the research and analysis of the relevant case-law. The employee in question must, in brief, be capable of examining and interpreting the provisions of the law by identifying the types of offences, as well as the applicability of these types of offences in the context of the company's operations. They must also understand the company's operations, knowledge gained in a position of responsibility and hierarchical context within the company and have the ability to translate into rules of conduct the processes outlined in the organisational Model dedicated to risk prevention.

Organisational expertise, i.e. specific preparation regarding the analysis of company procedures and organisational processes, as well as general principles on "compliance" legislation and related controls. At least one of the members of the Supervisory Board must have experience in preparing control procedures and manuals. The profile is therefore that of an internal control expert who has gained this experience in the context of activities that have long been "regulated" and "supervised".

Competence in the sector in which the Company carries out its characteristic management and/or with

experience in the activities most exposed to the risk of alleged offences.

The necessary autonomy of the Supervisory Board is guaranteed, due to its recognised position in relation to the departments mentioned in the context of the company organisational chart and the reporting lines assigned to them.

In order to assist in defining and carrying out the activities for which it is responsible and to ensure maximum compliance with the legal requirements and obligations, the Supervisory Board:

- avails itself of the Internal Audit department, where established, or an equivalent department, with adequate resources;
- may involve appropriate company resources to extract, process data and produce reports.

Grounds or (in)eligibility, removal and suspension of members of the Supervisory Board

The members of the Supervisory Board must meet the integrity requirements set out in Article 26 of the Legislative Decree of September 1, 1993, no. 385: in particular, those who find themselves in the situations stipulated by Article 2382 of the Italian Civil Code cannot be appointed as members of the Supervisory Board.

In addition, those who have been convicted by a sentence, even if not final, and even if issued under articles 444 and subsequent of the Code of Criminal Procedure and even in case of a conditionally suspended sentence, except for the effects of rehabilitation, cannot be appointed as a member of the Supervisory Board:

1) to imprisonment for a period of not less than one year for one of the crimes stipulated by the Royal Decree 267 of 16 March 1942;
2) to imprisonment for a period of not less than one year for one of the offences stipulated by the regulations governing banking, financial, securities and insurance activities and by the regulations governing markets and securities and payment instruments;
3) to imprisonment for a period of not less than one year for an offence against the public administration, against public faith, against public property, against the public economy, for a tax offence;
4) for any crime not punishable by imprisonment for a period of time not less than two years;
5) for one of the offences stipulated in Title XI of Book V of the Civil Code as reformulated by Legislative Decree no 61/2002;
6) for an offence which amounts to and has led to the conviction from which derives the prohibition, even temporary, to hold public offices, or the temporary prohibition to hold an executive position in legal persons and companies;
7) for one or several of the offences strictly stipulated by the Decree, even if with sentences lower than those indicated in the previous points;
8) those who have held the position of member of the Supervisory Board within companies to which the sanctions stipulated in art. 9 of the Decree have been applied;
9) persons to whom one of the prevention measures stipulated by Article 10, paragraph 3, of Law No. 575 of 31 May 1965, as replaced by Article 3 of Law No. 55 of 19 March 1990 and subsequent amendments, has been applied;
10) those against whom the accessory administrative sanctions stipulated by art. 187 quater of Legislative Decree no. 58/1998 have been applied.

Candidates for the office of member of the Supervisory Board must self-certify by means of a declaration in lieu of notoriety under Presidential Decreeno. 445/2000 that they do not find themselves in any of the situations listed under

numbers 1 to 10, expressly undertaking to communicate any changes in the content of these declarations.

The members of the Supervisory Board cease to hold office when they find themselves, after their appointment, in one of the situations indicated above.

Finally, those who are in one of the following situations may not be appointed, or shall be removed:

- *Conflicts of interest, including potential conflicts of interest, with the Company such as to prejudice the independence required by the role and tasks to be performed;*
- *Direct or indirect ownership of shares of such an importance as to enable them to exercise significant influence over the Company;*
- *Public employment in central or local government during the three years preceding the appointment as a member of the Supervisory Board.*

7.3 Functions and powers

The Supervisory Board defines and carries out the activities for which it is responsible according to the rule of collegiality and is endowed, under art. 6, paragraph 1, letter b) of Legislative Decree 231/2001 with "autonomous powers of initiative and control".

The activities that the Board is called on to perform are:

- Supervision of the **effectiveness** of the Model, which consists in verifying the consistency between the actual behaviours and the established Model;
- Examining the **adequacy** of the Model, i.e. its real (and not merely formal) capacity to prevent unwanted conduct in principle;
- Analysing the **maintenance** over time of the model's requirements of efficacy and functionality;
- Carrying out the **necessary dynamic updating** of the Model, in the event that the analyses carried out make it necessary to make corrections and adjustments. As a rule, this updating takes place in two distinct and integrated phases:
    - **Presentation of proposals to adapt the Model** to the corporate bodies/departments able to give them concrete implementation in the corporate fabric. Depending on the type and scope of the interventions, the proposals will be directed to the Personnel/HR and organisation, Administration departments, etc., or, in some cases of particular importance, to the Board of Directors;
    - **Follow-up**, i.e. verification of the implementation and effective functionality of the proposed solutions.

The Supervisory Board, making use of the powers attributed to it, is therefore specifically called on to primarily carry out the following activities:

- Establishing the control activities at each operating level, equipping itself with the informative or non-informative tools to promptly report anomalies and malfunctions of the Model by verifying and preparing control manuals, where necessary;
- Activating the control procedures by bearing in mind the need to streamline the procedures and the fact that

the primary responsibility for activity control is in any case entrusted to the Department Heads and/or to the top management of the company, to the corporate bodies appointed for this purpose and to the independent auditors;

- Updating the Model in accordance with the evolution of the regulations in force on the subject, as well as as a consequence of the changes in the company's internal organisation and activity;

- Collaborating in the preparation and integration of internal "regulations" (Codes of ethics and conduct, Procedures/operating instructions, Control manuals, etc.) dedicated to risk prevention;

- Adequately identifying, measuring and monitoring all the assumed risks or risks likely to be assumed as well as deriving from the interpretation and application of the reference standards, with respect to the actual company processes and procedures and with reference to the various operating segments of the company, constantly updating the risk detection and mapping activity;

- Promoting initiatives aimed at spreading knowledge of the Model among the bodies and employees of the company by providing any necessary instructions and clarifications, as well as by setting up specific training seminars;

- Coordinating with the other company departments to improve activity control and all matters regarding the concrete implementation of the Model;

- Carrying out extraordinary checks and/or targeted investigations when malfunctions of the Model are detected or when the offences covered by the prevention activities have been committed;

- Ensuring that the approved supervisory programme is drawn up, in line with the principles contained in Model 231, within the various sectors of activity; ensuring the coordination of the implementation of the supervisory programme and the implementation of planned and unplanned control measures.

In order to make the activity of the Supervisory Board feasible, it is necessary that:

- The activities carried out by the board may not be reviewed by any other body or corporate structure, without prejudice, however, to the fact that the governing body is in any case called on to supervise the adequacy of its intervention, since the governing body is ultimately responsible for the functioning and effectiveness of the organisational model;

- The Supervisory Board has free access to all the company departments without the need for any prior consent in order to obtain any information or data deemed necessary for the performance of the tasks stipulated by Legislative Decree 231/2001;

- Under its own direct supervision and responsibility, the board may use the assistance of all the company structures or external consultants.

In the context of the procedures for drawing up the company budget, the Supervisory Board will have at its disposal an allocation of financial resources, proposed by the board itself, which the Board will be able to use for any requirement necessary for the correct performance of its tasks (e.g. specialist consultancy, travel, etc.).

In carrying out the tasks assigned to it, the Supervisory Board has unrestricted access to company information for investigation, analysis and control activities. All corporate departments, employees and/or members of the corporate bodies are required to provide information in the event of requests from the Supervisory Board or the occurrence of events or circumstances relevant to the performance of the activities of the Supervisory Board.

7.4 Obligations to notify the Supervisory Board

The obligation to notify the Supervisory Board is a further instrument to facilitate the monitoring the Model's effectiveness and the subsequent assessment of the causes that made possible the occurrence of the offence.

This obligation is addressed to the company departments at risk of offences and concerns: a) the periodic results of the control activity they carried out to implement the models (summary reports of the carried out activity, monitoring activities, final indices, etc.); b) the anomalies or atypical cases found in the available information (a fact that is not relevant if considered individually, could have different relevance if repeated or if the area of occurrence is extended).

The above-mentioned information is sent to the Supervisory Board every six months (**ordinary information flows**), and concerns, for example:

- Decisions relating to the application, allocation and use of public funds;
- Statistics on workplace accidents with specification of the cause/reason, the occurrence, possible recognition of the accident and its severity;
- List of any pending lawsuits involving the Company (not already reported to the Supervisory Board in a timely manner);
- Commissions of inquiry or internal reports from which liability may theoretically emerge for the offences under Legislative Decree 231/2001;
- Summaries of contracts awarded following tenders at national and European level, i.e. by means of private negotiation;
- Information regarding contracts awarded by public bodies or persons performing functions of public utility.
- Any supplies requested exceptionally to suppliers listed in the 'Black List';
- Blocking of invoicing activities related to invoices exceeding the amount of 500,000.00 Euro without adequate documentary/contractual support;
- Any external inspection carried out by Public Officials, together with a brief description of the activity carried out.

In addition to the ordinary information flows referred to above, information regarding particular or specific situations and/or events, as specified below (extraordinary information flows), must also be provided to the **Supervisory Board in a timely and compulsory** manner:

- Measures and/or information from the judicial police or any other authority, from which you can infer that investigations are being carried out, even against unknown persons, for the offences under Legislative Decree 231/2001;
- Requests for legal assistance made by managers and/or employees in the event of initiation of legal proceedings for the offences stipulated in the Decree;
- Any fact, act, event or omission detected or observed in the exercise of the assigned responsibilities and tasks which present a risk with respect to compliance with the decree's provisions;
- Information on the actual implementation of the Organisational Model at all company levels, with evidence of the disciplinary proceedings carried out and of any sanctions imposed (including measures against Employees), or of the measures for the closure of such proceedings with the relevant reasons.

The Supervisory Board may propose any changes to the above-mentioned lists to the Chief Executive Officer. Any omission or delay in notifying the Supervisory Board of the information flows listed above will be considered a violation of the Organisational Model and may be sanctioned in accordance with the provisions of the Disciplinary System referred to in paragraph 9.2 below.

The information provided allows the Supervisory Board to improve its planning of controls and do not impose on it activities of timely and systematic verification of all the presented phenomena. In other words, the Board does not have an obligation to act whenever it receives information/reports, being left to its discretion and responsibility to establish in which cases to act.

7.5 Reports to the Supervisory Board by employees or company representatives or by third parties

Within the company, in addition to the documentation required by the procedures set out in this Model, any other information of any kind, originating from third parties and relating to the implementation of the Model in areas of activity at risk must be brought to the attention of the Supervisory Board.

In particular, the obligation to provide information is also extended to employees who come into possession of information relating to the commission of offences in particular within the company or who learn in the exercise of their functions of the perpetration of practices that are not in line with the rules of conduct that the company is required to issue (as seen above) within the scope of the Model specified in Legislative Decree 231/2001 (the so-called codes of ethics).

The obligation to inform one's employer of any conduct contrary to the Organisational Model is part of the broader duty of care and loyalty of the employee as per articles 2104 and 2105 of the Italian Civil Code.

These rules specify, respectively:

- "*The employee must use the diligence required by the nature of the service due, by the interest of the company and by the best interests of national production*";
- "*It must also comply with the provisions for the performance and discipline of the work imparted by the company and its collaborators on whom it is hierarchically dependent*". (art. 2104 Civil Code) and "*The employee must not carry out business activities, on his own behalf or on behalf of third parties, in competition with the company, nor disclose information relating to the company's organisation and production methods, or make use of them in such a way as to be prejudicial to it*". (Article 2105 Civil Code).

The specification of an effective reporting system guarantees confidentiality to those who report violations in accordance with Law no. 179 of 30 November 2017. At the same time, deterrent measures are provided against any improper information, both in terms of content and form.

In order to ensure a responsible management and in line with the legislative requirements, NTT DATA Italia S.p.A. has implemented a Whistleblowing system, adjusted to the regulatory changes introduced by Legislative Decree no. 24 of 10 March 2023, which transposed Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law and laying down provisions concerning the protection of persons who report breaches of national laws.

In general, the legislation on Whistleblowing is extensively regulated by Legislative Decree 24/2023 - to which reference is made -, which provides, as to the extent considered appropriate to highlight here:

- the possibility of reporting violations - i.e. conduct, acts or omissions detrimental to the interest of the entity - which are deemed to have been committed, including: (i) administrative, accounting, civil and criminal offences and (ii) unlawful conduct relevant under Decree 231, or violations of the organisation and management models;

- the identification of a person, a dedicated autonomous internal office or an external autonomous person to manage the reporting channel;

- the identification of specific channels, including electronic ones, for the internal reporting of violations, in written and/or oral form;

- the confidentiality and privacy of the information received and the protection of the personal data of the reporter and the reported person;

- precise timeframes for the initiation, performance and conclusion of the investigative activity carried out by the person handling the report;

- the prohibition of retaliation against the person making the report, i.e. of any conduct, act or omission, even if only attempted or threatened, put in place as a result of the report, which causes or may cause the reporting person, directly or indirectly, unjust damage;

- the nullity of any retaliatory measures taken against the reporting person;

- the provision of disciplinary sanctions: (i) for those who violate the confidentiality of the person making the report; (ii) for those who, with wilful misconduct or gross negligence, make unfounded reports (iii) in the event of retaliation against the person making the report; and (iv) in the event that the report is obstructed or there has been an attempt to obstruct it.

The Company has implemented a **specific procedure for whistleblower reports pursuant to Legislative Decree 24/2023**, published on the company intranet and available to all employees, to which full reference is made.

This procedure is an integrated part of the 231 Model.

7.6 Periodic checks and reports of the Supervisory Board

In order to guarantee the updating and efficiency of this Model, the Supervisory Board will carry out two types of checks:

- Document verification: annual verification of the main corporate documents and of the most important contracts concluded by the company in areas of risk activity in order to verify the compliance of the activities pertaining to them with the procedural and behavioural rules established by the Model;

- Verification of the Model: periodic verification of the Model's functioning and of the effective compliance with the conduct procedures established internally by the company for the prevention of crimes in the areas of activity exposed to the commission of crimes.

Following these verifications, the Supervisory Board draws up a special report, highlighting the identified risks and suggesting the actions to be taken, to be submitted to the attention of the Board of Directors, on an annual basis.

7.7 Proxy system

The Company adopts a system of power of attorneys and proxies - as described in paragraph 4.3 above - so that the strategy defined in the business plan and approved by the Board of Directors can be implemented by the organisational structure. The system of powers of attorneys and proxies reflects the hierarchy of roles.

The Supervisory Board may indicate any changes to be made to this policy/strategy in order to adapt it to the requirements of the Decree.

The indications provided by the Supervisory Board will be evaluated by the Board of Directors, which will autonomously adopt the appropriate decisions.

7.8 Information archiving

All information, notification and reports stipulated in the Model are kept by the Supervisory Board in a special computer and/or paper database. The data and information stored in the database are made available to persons outside the Supervisory Board with the prior authorisation of the Supervisory Board itself. The latter shall define the criteria and conditions for access to the database in writing.

8 MODEL DISSEMINATION AND IMPLEMENTATION

8.1 Communication plan

8.1.1 Communication to the members of the corporate bodies

The Model shall be brought to the attention of the Corporate Secretarial office of each corporate body who - due to their appointment or absence - has not already taken part in the approval of the Model.

8.1.2 Communication to Executives and Department Managers

On the instructions of the Supervisory Board, the principles and contents of the Model are formally communicated by the Management to all managers (in office and per position) and to the Department Managers, through delivery of this document and/or distribution on the company intranet.

8.1.3 Communication to all other employees

This document is sent/made available in electronic form to all employees and is available for consultation on the website (also available to third parties), as well as on the company intranet.

In order to encourage the Model's dissemination to all employees, within the personnel departments, the Department

Managers and the management functions have the task of communicating and underlining the importance of the values, rules and instruments that make up the Model itself.

8.1.4 Personnel training

Personnel training for the purposes of implementing the Model is managed by the Human Resources Manager in close collaboration with the Legal & Compliance department and the Supervisory Board. The principles and contents of Model 231 are also disseminated through training courses in which the persons identified above are required to participate. The structure of the training courses is defined by the Head of Human Resources/Human Resources together with the Legal & Compliance department and with the advice of the Supervisory Board.

The following training tools are also used:

- Periodic note Internal information;
- Information in the letters/documents in the recruitment phase for newly hired employees (e.g. "Welcome Kit/Your Guidebook" or similar tool);
- Intranet access;
- Circular letter also sent by mail/email.

8.2 Communication to third parties

Information may be provided to parties outside NTT DATA Italia (for example: Representatives, Consultants and Business Partners) on the policies and procedures adopted by the company on the basis of this Organisational Model, as well as the texts of the contractual clauses normally used in this regard.

The commitment to comply with the reference principles of Model 231 on the part of third parties having contractual relationships with NTT DATA Italia is in fact stipulated by means of a specific clause in the relevant contract, which is accepted by the third party, with termination *ipso jure* in the event of non-compliance.

8.2.1 Training of external collaborators

The external collaborators which NTT DATA Italia could involve in the development and management of projects due to the need for know-how or the unavailability of internal resources, must be aware of the provisions of Legislative Decree 231/2001 and, where required, declare that they have adopted Model 231 or, at least, appropriate procedures to avoid in any way the involvement of NTT DATA Italia in the event of the commission of the offences stipulated by the above-mentioned legislation.

9 DISCIPLINARY SYSTEM

9.1 General principles and criteria for imposing sanctions

The disciplinary mechanisms indicated herein form an integral part of the Company's organisational model.

In general, the application of disciplinary sanctions does not depend on whether or not criminal proceedings for the commission of one of the offences stipulated in Legislative Decree 231/2001 have been initiated and concluded. 231/2001.

In individual cases, the application of specific sanctions is defined and applied in proportion to the severity of the assessed non-compliance, in accordance with the general principles governing labour law.

In individual cases, the type and extent of specific penalties is applied in proportion to the severity of the non-compliance and, in any case, on the basis of the following general criteria which may be cumulated:

a) subjective element of the conduct (wilful misconduct or negligence, the latter due to imprudence, negligence or inexperience also in view of the event's predictability or lack of);

b) importance of the breached obligations;

c) gravity of the danger created;

d) recidivism in the two-year period;

e) the extent of any damage caused to the Company by the possible application of the sanctions stipulated by Legislative Decree 231/2001 and subsequent amendments and additions;

f) level of hierarchical and/or technical responsibility;

g) presence of aggravating or mitigating circumstances, with particular regard to previous work performance and previous disciplinary actions in the last two years;

h) sharing of responsibility with other workers who have contributed to the non-compliance;

i) where more than one offence has been committed by a single act and is punishable by different penalties, the most serious penalty shall apply;

j) recidivism in the two-year period automatically entails the application of the most serious sanction within the foreseen typology;

k) the principles of timeliness and immediacy require the imposition of disciplinary sanctions, irrespective of the outcome of any criminal proceedings.

RECIPIENTS

This disciplinary system is divided by category of recipients, under Article 2095 of the Italian Civil Code, as well as the possible autonomous or parasubordinate nature of the relationship between the recipients themselves and the Company and refers to:

a) persons who hold positions of representation, administration or management of the Company (so-called "*Executives*");
b) persons subject to the management or supervision of one of the above mentioned persons (so-called "*Employees*"), as well as to the persons referred to in paragraph 9.2.4 (the so-called), "*External collaborators*).

In any case, the imposition of the sanction implies the involvement of the Supervisory Board, which assesses the existence and seriousness of the violation.

9.2 Penalties

9.2.1 Penalties for employees (Executives - employees)

1. SCOPE OF APPLICATION

Under the combined provisions of Articles 5(b) and 7 of Legislative Decree 231/2001, without prejudice to the prior contestation and the procedure prescribed by art. 7 of Law no. 300 of 20 May 1970 (the so-called Employees' Statute), the sanctions stipulated in this Section apply to executives and employees of the Company who commit disciplinary offences deriving from:

a) failure to comply with the procedures and requirements contained in the Organisational Model due to serious non-compliance with the provisions aimed at guaranteeing the performance of the activity in compliance with the law and at promptly discovering and eliminating risk situations, under Legislative Decree 231/2001;

b) serious or repeated violation of the internal procedures contained in the Organisational Model, by behaving in such a way as to tolerate significant irregularities or to omit to carry out the controls and/or checks provided for in the individual procedures, even if the Company's interests have not been prejudiced;

c) violation and/or circumvention of the internal control system, carried out by removing, destroying or modifying the procedure documentation or by preventing the control of or access to the information and documentation to the persons in charge, including the Control Body;

d) serious or repeated failure to comply with the rules contained in the Code of Ethics;

e) repeated failure to comply with the obligation to inform the Control Body and/or the direct hierarchical superior of the failure to comply with the procedures and requirements of the Organisational Model;

f) conduct aimed at committing an offence stipulated by Legislative Decree 231/2001 and subsequent amendments and additions.

2.SANCTIONS

Failure to comply with the procedures and requirements contained in this Section of the Disciplinary System, paragraph 1 letters a) to f) by executives and employees, depending on the seriousness of the offence, is sanctioned with the following disciplinary measures indicated per levels and in full compliance with the applicable Collective Labour Contracts:

(a) verbal reprimand;

(b) written reprimand;

(c) a fine not exceeding the amount of three hours' pay;

(d) suspension from work;

(e) dismissal with notice;

(f) dismissal without notice.

If the above-mentioned employees have a power of attorney with the power to represent the Company externally,

the imposition of the most serious sanction of the fine will also result in the automatic revocation of the power of attorney.

2.A) Verbal reprimand

The sanction of a verbal reprimand is imposed in cases of negligent and slight violation of the procedures and/or requirements contained in the Organisational Model as well as of the rules contained in the Code of Ethics that have no consequences for the Company.

2.B) Written Reprimand

The sanction of a written reprimand is imposed in case of:

a) recidivism in the two-year period in cases of willful misconduct violation of procedures and/or requirements contained in the Organisational Model, as well as of the rules contained in the Code of Ethics;

b) minor procedural errors due to negligence on the part of the worker having external significance.

2.C) FINES

In addition to the cases of recidivism in the commission of the offences referred to in letter b) of point 2 b) above, a fine may be applied in cases where, due to the level of hierarchical or technical responsibility, or in the presence of aggravating circumstances, willful misconduct and/or negligent behaviour may undermine, albeit at a potential level, the effectiveness of the Organisational Model; such as, by way of example but not limited to:

a) failure to comply with the obligation to inform the Control Body and/or the direct hierarchical or functional superior of the failure to comply with the procedures and requirements of the Organisational Model;

b) failure to comply with the requirements of the procedures and rules indicated in the Organisational Model, as well as with the rules contained in the Code of Ethics, in the event that they concerned or concern a procedure of which one of the necessary parties is the Public Administration.

2.D) SUSPENSION FROM OFFICE

The sanction of suspension from office is imposed, as well as in cases of recidivism in the commission of offences which may result in the application of the fine, in cases of serious violations of procedures and requirements contained in the Organisational Model as well as of the rules contained in the Code of Ethics such as to expose the Company to risks and responsibilities under Law 231/01.

2.E) DISMISSAL WITH NOTICE

The sanction of dismissal with notice is imposed in cases of repeated serious violation of the procedures and requirements contained in the Organisational Model and of the rules of the Code of Ethics having external relevance in the performance of activities in the areas/activities at risk of crime under Legislative Decree 231/2001 and subsequent amendments and additions.

2.F) DISMISSAL WITHOUT NOTICE

The sanction of dismissal without notice is imposed for such serious misconduct as not to allow the continuation, even on a provisional basis, of the employment relationship (so-called just cause) such as, by way of example, but

not limited to:

a) a conduct aimed at committing an offence included among those stipulated in and subsequent amendments and additions;

b) violation and/or fraudulent circumvention of procedures and requirements contained in the Organisational Model and of the rules of the Code of Ethics having external relevance for the purpose of committing or facilitating crimes under Legislative Decree 231/2001 and such as to eliminate the fiduciary relationship with the employer;

c) violation and/or circumvention of the internal control system, carried out by removing, destroying or altering the procedure documentation or by preventing the control of or access to information and documentation to the persons in charge, including the Control Body in order to commit, contribute to or facilitate crimes under Legislative Decree 231/2001 and in such a way as to prevent If the worker has committed one of the offences stipulated in this article, the Company may decide the precautionary dismissal with immediate effect.

The Human Resources/Personnel Department communicates the enforcement of the sanction to the Supervisory Board. The disciplinary system is constantly monitored by the Supervisory Board and the Human Resources/Human Resources department.

All legal and contractual obligations relating to the imposition of disciplinary sanctions are complied with.

9.2.2 Measures against Executives

1.SCOPE OF APPLICATION

Under the combined provisions of Articles 5(b) and 7 of Legislative Decree 231/2001, and, limited to these rules, in compliance with the procedure stipulated in art. 7 of Law no. 300 of 20 May 1970, the sanctions indicated in this Section apply to executives who commit disciplinary offences deriving from:

a) violation of the internal procedures contained in the Organisational Model by behaving in a way that consists in tolerating irregularities in work or in not complying with work duties or obligations even in the event that there has been no prejudice to the Company's activity or interests;

b) serious non-compliance with the procedures and requirements contained in the Organisational Model such as to involve situations of risk, under Legislative Decree 231/2001;

c) violation and/or circumvention of the internal control system, carried out by removing, destroying or altering the procedure documentation or by preventing the control or access to information and documentation to the persons in charge, including the Control Body, in order to commit, contribute to or facilitate crimes under Legislative Decree 231/2001;

d) serious breach of the rules contained in the Code of Ethics;

e) repeated failure to comply with the obligation to inform the Control Body and/or the direct hierarchical superior of the failure to comply with the procedures and requirements of the Organisational Model;

f) serious or repeated failure to supervise as "hierarchical manager" the compliance with the procedures and requirements of the Organisational Model by their subordinates in order to verify their actions within the areas

at risk of crime and, in any case, in the performance of activities instrumental to operational processes at risk of crime.

2.SANCTIONS

In the event of failure to comply with the procedures and requirements contained in this Section of the Disciplinary System paragraph 1 letters a) to h), depending on the seriousness of the offence, the most appropriate measures will be applied against those responsible in accordance with the provisions of the applicable National Collective Work Agreement for Executives. Specifically:

- in the event of a minor violation of one or several procedural or behavioural rules set out in the Model, the manager shall be required in writing to comply with the Model, which is a necessary condition for maintaining the relationship of trust with the Company;
- in the event of a serious or repeated violation of one or several provisions of the Model such as to constitute a significant breach, the manager shall be dismissed with notice;
- where the violation of one or several provisions of the Model is so serious as to irreparably damage the relationship of trust, not allowing the continuation, even temporary, of the employment relationship, the employee shall be dismissed without notice.

If the manager has a power of attorney with the power to represent the Company externally, the imposition of the disciplinary sanction will also result in the automatic revocation of the power of attorney.

9.2.3 Measures against "Top Management" and Statutory Auditors

1. SCOPE OF APPLICATION

For the purposes of Legislative Decree 231/2001, in the current organisation of the Company the following persons are considered *"Top Management":*

- the Managing Director;
- The Directors with legal representation;
- the other Directors;
- the General Directors, if appointed.

Under the combined provisions of Articles 5(a) and 6 of Legislative Decree 231/2001 the sanctions stipulated in this Section shall apply to *"Top Management"* in the following cases:

a) serious or repeated failure to comply with the specific protocols (procedures and requirements) stipulated in the Organisational Model under Legislative Decree 231/2001, aimed at planning the formation and implementation of the Company's decisions in relation to the crimes to be prevented, and the rules contained in the Code of Ethics, including the violation of the provisions relating to the powers of signature and, in general, the system of proxies as well as the violation of the measures regarding the management of financial resources;

b) violation and/or circumvention of the internal control system stipulated in the Code of Ethics and in the Organisational Model, by removing, destroying or altering the documentation stipulated in the protocols (procedures and requirements) or by preventing the control of or access to information and documentation by the persons in charge, including the Control Body;

c) serious or repeated violation of the disclosure obligations stipulated in the Organisational Model towards the Supervisory Body and/or any supervised person; failure, in the exercise of the hierarchical powers and within the limits deriving from the system of proxies, to comply with the obligations of control and supervision of the behaviour of the direct subordinates, meaning only those who, under the direct and immediate authority of the top management, operate within the areas at risk of crime.

2. PROTECTION MEASURES

Depending on the seriousness of the offence committed by the Director, the Board of Directors, having heard the opinion of the Board of Statutory Auditors, will take the most appropriate measures, including the revocation of the transactions falling within the scope of the proxies, the modification or revocation of the proxies themselves and in the most serious cases, convening the Shareholders' Meeting for the adoption of the measures under Articles 2383 and 2393 of the Italian Civil Code.

If the reported violation is committed by two or several members of the Board of Directors, if it considers the report received from the Control Body to be justified and the Board of Directors has not done so, the Board of Statutory Auditors shall convene the Shareholders' Meeting under Article 2406 of the Italian Civil Code and, once the existence of the violation has been ascertained, it shall adopt the most appropriate measures, including, in the most serious cases, those under Articles 2383 and 2393 of the Italian Civil Code.

3. COEXISTENCE OF SEVERAL RESPONSIBILITIES OF THE SAME PERSON

In the event that the top management employee also holds the position of manager, in the event of violations carried out as top management, the sanctions of this Section will be applied to him, without prejudice, however, to the applicability of the various disciplinary actions applicable on the basis of the employment relationship with the Company and in compliance with the legal procedures, where applicable.

4. MEASURES AGAINST AUDITORS

In the event of violations committed by one or several Statutory Auditors, the Supervisory Board informs the Board of Directors and the Board of Statutory Auditors, so that they can proceed without delay and in accordance with the powers stipulated by law and/or the Articles of Association, to convene the Shareholders' Meeting to reach the necessary resolutions, which may also consist in revoking the appointment for just cause.

9.2.4 External collaborators

1. SCOPE OF APPLICATION

With regard to those who, in their capacity as collaborators, consultants and suppliers of NTT DATA Italia, are therefore required to comply with the obligations set out in Legislative Decree 231/2001, have committed the serious violations of the rules of the Code of Ethics and of the procedures and requirements contained in the Organisational Model indicated below, the termination of the contractual relationship for legal grounds may be decided under art. 1456 of the Italian Civil Code.

This is without prejudice, in any case, to any claim submitted by the Company for compensation for damages suffered.

2. NON-COMPLIANCE

a) fraudulent circumvention of company procedures and requirements and of the rules of the Code of Ethics concerning the object of the assignment having external relevance or violations carried out by means of conduct aimed at committing an offence included among those stipulated in Legislative Decree 231/2001 and the subsequent amendments and additions;

b) lack of, incomplete or untrue documentation of the activity carried out, subject of the assignment, such as to prevent its transparency and verifiability.

3. CONTRACTUAL CLAUSES

The following is the text of the clause to be included - with the appropriate modifications - in the Orders to third party suppliers, in the contracts and in the Internal Covenants of the temporary companies consortia (RTI / ATI):

*"With specific reference to Legislative Decree no. 231/2001 and subsequent amendments and additions. (**"Decree 231"**) and for the purposes of prevention and repression of willful misconduct criminal offences stipulated and reported in it (**"Assumed Offences"**), the Supplier, the Collaborator and/or the third party supplier, having a business relationship with NTT DATA Italia under this Contract (the **"Supplier"**), declares it has been made aware and undertakes to comply with the key principles reflected in the Code of Ethics and Professional Conduct of NTT DATA EMEAL available on the NTT DATA Italia website https://it.nttdata.com/Conoscici/NTT%20DATA_CC_IT.pdf ("**Code of Ethics"**), including the fight against corruption and counterfeiting of intellectual and industrial property assets, and also undertakes to comply with the minimum standards of conduct specified in the Code of Ethics (collectively the **"Core Principles"**).*

The supplier also declares that he has read the Organisational Model (General Section) of NTT DATA Italia, which can be consulted on the website and/or on the Supplier Portal.

*In view of the above-mentioned facts, the supplier is aware that (a) the failure to comply or the partial failure to comply with the Basic Principles of the Code of Ethics and/or (b) the indictment for one of the alleged offences stipulated in Decree 231 (where they are punishable for willful misconduct) will constitute a serious breach of contract and will entitle NTT DATA Italia to **terminate this Contract ipso jure** under and for the purposes of Article 1456 of the Italian Civil Code, within the deadlines set out in this clause, without prejudice to claiming compensation for any damages caused to the Company.*

9.2.5 Measures to protect reports (Whistleblowing)

The Whistleblowing Decree provides for the establishment of a system of sanctions against persons responsible for the offences indicated below.

1. Malicious or negligent whistleblowing

Without prejudice to the provisions of the Whistleblowing Decree, if, upon analysis of the report, it emerges that the report is unfounded and it is ascertained that the reporting person made the report with wilful misconduct or gross negligence, the sanctions provided for by the Model shall be applied.

Disciplinary sanctions shall be imposed on the reporting person, taking into account, by way of example:

- the seriousness of the subjective element, i.e. the existence of wilful misconduct or gross negligence by the person making the report which turns out to be unfounded;
- the seriousness of the facts falsely reported;
- the use of fraudulent means (e.g. falsification of evidence).

This is without prejudice, in any case, to any assessment of the appropriateness of filing a complaint or a lawsuit in the case of acts or facts of criminal relevance.

2. Breach of the confidentiality of the whistleblower

Any breach of the confidentiality of the reporter will be considered to apply the sanctions provided for in the Model.

In such a case, it should be taken into account, by way of example and not exhaustively:

- whether the disclosure was made intentionally or by mistake;
- the manner in which the disclosure was made and its dissemination;
- whether the disclosure has exposed the whistleblower to risks.

3. Other wrongdoing

The sanctions provided for by the Model shall be applied if one of the following offences has been detected:

- retaliation was committed against the whistleblower;
- the report was obstructed or an attempt was made to obstruct it.