POLICY FOR THE PREVENTION OF FRAUD AND VIOLATIONS OF THE CODE OF ETHICS AND FOR THE MANAGEMENT OF "WHISTLEBLOWING" REPORTS

Company:

Esprinet S.p.A., V-Valley S.r.l., Dacom S.p.A.

Facility:

All facilities

Subsystem:

Legislative Decree No. 231/01, Regulation 2016/679, Legislative Decree 24/23

File name:

DIS01001 Policy for the prevention of fraud and infringements of the Code of Ethics and for the management of "Whistleblowing" reports

Responsibility for the document:

Version	Date	Version Note	Edited by	Checked	Approved
00	01/03/16	First issue	P. Aglianò CRO	G. Monina HIA	A. Cattani CEO
01	15/10/18	Whistleblowing update	P. Aglianò CRO	G. Monina HIA	A. Cattani CEO
02	29/06/21	Update	P. Aglianò CRO	G. Monina HIA	A. Cattani CEO
03	16/03/22	Extension to V-Valley Advanced Solutions España	P. Aglianò CRO	G. Monina HIA	A. Cattani CEO
04	08/06/22	Extension to Dacom S.p.A.	P. Aglianò CRO	G. Monina HIA	A. Cattani CEO
05	03/07/23	Updating of the document intended to transpose the regulatory changes introduced by Legislative Decree 24/2023	P. Aglianò CRO	G. Monina HIA	A. Cattani CEO

CONTENTS

1. PURPOSE AND SCOPE

This policy summarizes the principles dictated by the Company for the purpose of effectively preventing and countering fraudulent and illegitimate conduct and in any case conduct contrary to the Code of Ethics, the Organizational Model pursuant to Legislative Decree 231/01, laws and Regulations, by all employees of the Italian companies of the Esprinet Group.

In addition, this policy deals with reports, of conduct that harms the public interest or the integrity of the private entity, relating to:

- offenses that fall within the scope of the European Union or national acts indicated in the annex to Legislative Decree 24/2023;
- acts or omissions that harm the financial interests of the Union or the internal market;
- acts or conduct that frustrate the object or purpose of the provisions set forth in Union acts in the aforementioned areas.

The strict application of these principles cannot be separated from the heartfelt participation of everyone, at all levels, with the assumption that internal control can only be effective through the contribution of all company functions, employees and collaborators, as well as of the control and support functions.

Its content is inspired by the principal international *best practices* in the field of internal control, above all, the CoSo-ERM system.

This procedure monitors the behaviour of the recipients, as defined below, in order to prevent the committing of offences and acts, as indicated above or of one or more offences provided by Legislative Decree. 231/01 and of the Criminal Code and to comply with the legislation on the protection of personal data. In particular, this procedure aims to:

- identify the tasks and responsibilities of the management/departments/organisational units involved;
- adjust and identify the traceability of the checks carried out;
- minimise the risk of committing crimes pursuant to Legislative Decree 231/01 and the Criminal Code;
- ensure compliance with current legislation and the system of company procedures;
- respect the principle of privacy *by default* and *by design* provided by Regulation (EU) 2016/679 of 17 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data;
- guarantee compliance with the principle of confidentiality, integrity, availability and traceability of information.

2. RECIPIENTS

This policy applies to all *i)* employees, self-employed workers and staff who carry out their activity at (not necessarily on behalf of) the Italian companies of the Esprinet Group; *ii)* volunteers and trainees, paid and unpaid, *iii)* freelancers and consultants who carry out their activity at (not necessarily on behalf of) the Italian companies of the Esprinet Group; *iv)* shareholders and persons with administrative, management, control, supervisory or representative functions, even if these functions are exercised purely as a matter of fact of the Italian companies of the Esprinet Group.

It will be the responsibility and duty of each function head to disseminate the principles, including among suppliers, consultants and occasional collaborators.

The protection of reporting persons also applies if the reporting takes place in the following cases:

- when the legal relationship (e.g. employment relationship, collaboration, consultancy, supply, etc.) has not yet begun, if the information on the infringements was acquired during the selection process or at other pre-contractual stages;
- during the trial period:
- after the dissolution of the legal relationship, if the information on the infringements was acquired during the course of the relationship itself.

3. TERMS AND DEFINITIONS

ABUSE	Any conduct that causes or is potentially likely to cause harm to the company, to the advantage or direct or indirect benefit of others, characterised by the distorted use of the trust granted and the circumvention of company rules.
COSO ERM	The COSO ERM is defined as a process implemented by the company's top management, aimed at identifying those potential factors that can exert a significant influence on the organisation, for managing risk within the "appetite" levels of the organisation and providing reasonable assurance regarding the achievement of company objectives.
PUBLIC DISCLOSURE	Placing information on infringements in the public domain through print or electronic media or otherwise, through means of dissemination capable of reaching a large number of people.
MANAGING ENTITY FOR NOTIFICATIONS	The management and verification of the well-foundedness of the circumstances represented in the notification are entrusted to the HIA and to the Chairman/Single Member of the Supervisory Board, who shall do so in accordance with the principles of impartiality and confidentiality, carrying out any activity regarded as appropriate, including the personal hearing of the whistleblower and any other persons who may report on the notified facts, with the adoption of the necessary precautions.
FACILITATOR	Natural person who assists the whistleblower in the reporting process, operating within the same working context and whose assistance must be kept confidential.
RISK FACTOR	Element that can lead to an increase in the probability of spreading fraudulent and disloyal behaviour that acts on one of the components of the fraud triangle.
FRAUD RISK ASSESSMENT	This is the assessment of the risks of fraud that not only permits a determination of "what" could cause fraud and its impact on society, but an understanding of the effectiveness of the measures.
FRAUD	Any event deriving from human conduct, characterised by fraud, i.e. by a false representation of reality, or by the distorted use of the trust granted or by the circumvention of company rules that causes or is potentially likely to cause a loss to the company, aimed at achieving a direct or indirect advantage or benefit for the perpetrator or for others.
EXTERNAL FRAUD	Fraud against Esprinet Group companies, committed by parties external to the organisation (customers, suppliers, third parties).
INTERNAL FRAUD	Fraud against Esprinet Group companies, committed by subjects internal to the organisation (employees).
MIXED FRAUD	Fraud against a company, committed on account of the complicity between subjects external and internal to Esprinet (e.g. agreement between the Purchasing Department and suppliers).
RISK INDICATOR	An element, the change in which is symptomatic of an increase in the level of risk (e.g. increase in "out-of-procedure" operations).
ANOMALY INDICATORS	Sign of a potential fraud requiring further investigation. (e.g. reimbursement of abnormal expenses, abnormal fuel consumption, etc.).
ANTI-FRAUD KPI	Performance indicator referring to one or more anti-fraud controls (e.g. decrease in inventory differences).
INVOLVED PERSON	Natural or legal person mentioned in the internal or external notification or in the public disclosure as the person to whom the infringement is attributed or as a person in any case involved in the infringement that is publicly reported or disclosed.
RED FLAG	Relevant indicators of potential fraud or abuse, constituting grounds for initiating an audit.
RETALIATION	Any conduct, act or omission, even if only attempted or threatened, carried out on account of the report, the complaint to the judicial or accounting authority

	or public disclosure, which causes or may cause an unfair loss to the whistleblower or the person who filed the complaint, whether directly or indirectly. By way of example, forms of retaliation include: • dismissal or suspension; • demotion or non-promotion; • change in duties, change of workplace, reduction of salary, change in working hours; • suspension of training; • imposing or administration of disciplinary measures, note of reprimand or other sanction, including pecuniary; • coercion, intimidation, harassment or ostracism; • non-renewal or early termination of a fixed-term employment contract; • discrimination, disadvantageous or unfair treatment; • demanding results that are impossible to achieve in the indicated manner and within the indicated time; • an artificially negative performance assessment; • unjustified revocation of appointments; • unjustified failure to confer tasks with simultaneous attribution to another person; • repeated rejection of requests (e.g. holidays, leave); • unjustified suspension of patents, licenses, etc.
WHISTLEBLOWER(S)	A person who makes a notification or a public disclosure, who belongs to one of the following categories: • employees of the Esprinet Group and those who work on the basis of relationships that determine their inclusion in the company organisation, including in a form other than an employment relationship; • shareholders and persons with administrative, management, control or supervision functions or of representation of members of the corporate bodies of the Esprinet Group; • non-employee workers (e.g. freelancers and consultants) who provide goods or services to the Esprinet Group.
BREACHES/ OFFENCES	Behaviour attributable to: • relevant offences pursuant to Legislative Decree 8 June 2001, No. 231, or non-compliance with organisational and management models; • offences falling within the scope of Union law, in relation to specific sectors (for example: financial services, products and markets and prevention of money laundering and terrorist financing; protection of the environment; protection of privacy and protection of personal data; security of networks and information systems); • acts or omissions that harm the financial interests of the European Union; • acts or omissions concerning (Art. 26, para. 2 of the TFEU) the free movement of goods, persons, services and capital in the internal market, including breaches of European Union competition rules; State aid; corporate taxes; • acts or conduct that defeat the object or purpose of the provisions of the European Union.
WHISTLEBLOWING	Reporting system whereby the worker who, while working within a company, detects a possible fraud, infringement, offence, irregularity, danger or other serious risk that may harm customers, colleagues, shareholders, the public or the integrity and reputation of the company/public body/foundation and decides to make the notification.
For the following definitions, see also the "report on corporate governance and ownership structures" pursuant to Article 123-bis of the Consolidated Law on Finance (TUF), available for consultation on the Esprinet – *Investor Relations* Area institutional website.	
CRC	Control and Risks Committee

BoD	Board of Directors
CEO	Chief Executive Officer
AI	Executive director for the internal control system
ANAC	Italian Anti-Corruption Authority
HIA	Head of *Internal Audit*
BSA	Board of Statutory Auditors
CRO	*Risk Manager*
ICRMS	Acronym for Internal Control and Risk Management System. This is defined as a set of rules, behaviours, policies, procedures and organisational structures that aim to enable the main operational risks to be identified, measured, managed and monitored, thereby helping to safeguard the Company's assets, the efficiency and effectiveness of company processes, the reliability of financial information, compliance with laws and regulations and with the articles of association and internal procedures.
SB	Supervisory Board

4. ACTIONS CONSTITUTING FRAUD

Fraudulent conduct and conduct contrary to the Code of Ethics must be understood as all those intentional actions carried out in circumvention of company rules or abusing the trust granted, with the aim of obtaining an unfair advantage. Fraud is defined as the misrepresentation of a material fact (or of the distorted use of the trust granted) to secure an advantage to the agent or a third party, whether directly or indirectly,.

By way of example and without limitation, the following illegal activities constitute corporate fraud:

- theft of property of the Esprinet Group;
- falsification or alteration of documents;
- falsification or manipulation of accounts and intentional omission of records, events or data;
- destruction, concealment or inappropriate use of documents, archives, furniture, installations and equipment;
- misappropriation of money, securities, supplies or other assets belonging to the Esprinet Group;
- giving of a sum of money or granting of another benefit to a public official as consideration for an official act (e.g. streamlining of customs procedures) or for the omission of an official act (e.g. failure to submit a report of dispute for tax irregularities);
- acceptance of money, goods, services or other benefits as incentives for favouring suppliers/companies;
- falsification of expense reports (e.g. "inflated" reimbursements or for false transfers);
- falsification of attendance at work;
- disclosure of confidential and proprietary information of the Esprinet Group to external parties (e.g. competitors);
- use of the organisation's resources and assets for personal use, without authorisation.

5. REFERENCES

LAWS AND REGULATIONS	Legislative Decree No. 231/01
	Legislative Decree No. 196/2003
	Legislative Decree No. 151/2015
	National Collective Labour Agreement for the Commercial Sector (CCNL)
	Law No. 300/1970 (Workers' Statute)
	GDPR (Regulation 2016/679 of 17 April 2016 on the protection of individuals with regard to the transfer of personal data, as well as on the free movement of such data).
	Code of Ethics
	Legislative Decree No. 24/2023
INTERNAL PROCEDURES AND DOCUMENTS	Internal disciplinary system
	Model "231", adopted by the Esprinet Italia Group
	Internal Regulations for the Use of IT Tools
	Procedure for Giveaways of Goods
	Procedure for the management and approval of Transactions with Related Parties
	Management of Gifts, Donations and Sponsorships
	Management of Audit Visits
	Esprinet Group Image Detection Systems Management Procedure
	Expense report procedure
	Guidelines for the Internal Control and Risk Management System
	Procurement and tender management procedure
	Esprinet Group Privacy Assignments Job Description
	Internal rules for *Internal dealing*
	Internal Regulations on Insider Information

6. ROLES AND RESPONSIBILITIES

6.1. CHIEF EXECUTIVE OFFICERS

The Chief Executive Officers (or the corresponding functions in the various Italian companies of the Group) shall confer an extensive commitment to the operational functions delegated to the management of the fraud prevention system and to the verification of reports of suspicious cases and shall take note of the activities carried out, the measures implemented and the cases ascertained in the half-yearly reports drawn up by the HIA.

In addition:

- they shall be promptly informed by the Supervisory Body in the most serious cases involving senior managers, members of the Supervisory Body or other members of the Supervisory Body or that in any case may cause serious impacts or affect the correct management of the company;
- they shall take measures in the cases described in the previous point.

6.2. CHIEF RISK OFFICER

The CRO defines the guidelines of this policy, identifying the risks of fraud in the *fraud risk assessment* phase, with the other operational, *compliance* and *financial report*-related risks, and presents the same and any updates or changes to the Control and Risk Committee.

Particular attention should be paid to the assessment of the tax impacts of acts of fraud.

In addition, he or she verifies the consistency of the specific fraud risk assessment criteria with the more general risk analysis methodologies and the company's *Risk Appetite Framework* (RAF).

6.3. CONTROL AND RISKS COMMITTEE

The CRC examines the policy presented by the CRO and proposes any changes and additions to it. The committee monitors work performed, measures implemented and cases detected during committee meetings which are attended by the HIA.

With respect to the reporting of significant events, the CRC shall be promptly informed by the Supervisory Board in more serious cases involving senior management, members of the Board of Statutory Auditors or other members of the Supervisory Board, or of events that could have a serious impact on or that involve the correct management of the Company.

6.4. INTERNAL AUDIT

The *Internal Audit* office:

- conducts in depth investigations of notifications;
- if, while carrying out its audit activities, the office becomes aware of potential acts of corruption, it shall make a preliminary assessment and notify these to the Supervisory Board.
- Its periodic report to the Board of Directors shall incorporate the progress of the fraud prevention system and any measures taken.

6.5. HUMAN RESOURCES

The Head of Human Resources:

- proceeds without delay with the elaboration of the disciplinary dispute and the investigation of the associated procedure in the event of receipt by the Supervisory Body, and the Chief Executive Officers of evidence of facts of disciplinary relevance to an employee. In the event of criminally significant offences that result in the filing of a denunciation or complaint, but which do not constitute independent disciplinary infringements, the Human Resources Manager shall immediately issue a formal notice, while assessing on a case-by-case basis whether or not to suspend the disciplinary proceedings until the criminal proceedings have been defined.

6.6. LEGAL DEPARTMENT

The in-house Lawyer:

- assesses the criminal significance of the evidence that emerges during the examination and in depth investigation phase for notifications of presumed frauds or infringements of the Organisational Model or the Code of Ethics, verifying, with the assistance of external legal counsels, whether the offence may be prosecutedex officio or following a complaint by one of the parties. In this latter event, the in-house lawyer shall submit any formal legal complaints to the Chief Executive Officer for signing and shall file these with the Judicial Police or competent Judicial Officers through external lawyers.

6.7. HEADS OF DEPARTMENT

Heads of Department constitute the first level of verification and shall constantly recall that by their example they can effectively contribute to the dissemination of virtuous conduct and respect for company values and rules, with regard to which they will not fail to raise awareness among their own staff at every favourable opportunity.

They are required:

- to notify the SB of any suspected infringement of the Organisational Model or the Code of Ethics, company rules and procedures or conduct that may constitute fraud and unlawful conduct, taking prompt action to prevent the continuation of conduct harmful to the company and, if such conduct falls within the scope of application of infringements/illegal conduct, to formalise such reporting through the *whistleblowing channels* indicated below;
- to keep confidential the identity of any employees who report to them any of the actions described in the preceding point;
- to avoid discriminatory or vexatious conduct towards those individuals who notify any of the acts described in the preceding points;
- to notify situations of conflict of interest personal to themselves or to their collaborators in timely fashion, including those concerning their family members, refraining from making decisions or intervening in any case in decision-making processes that may include such situations;
- not to use company information for private purposes;

- to behave fairly and impartially;
- to distribute the workload equally among their staff, on the basis of skills, attitudes, professionalism and respect for duties;
- to express impartial assessments of staff;
- to spread awareness of good practices and good examples, strengthening the sense of trust in and belonging to the company.

7. RISK ASSESSMENT

The risk of fraud and of conduct contrary to the Code of Ethics is of a cross-cutting nature, insofar as it may have impacts not only on capital losses but also on the corporate image and the normal conduct of operations. For an effective risk assessment, therefore, the following must be taken into account:

- direct losses (material value of the company asset affected and/or sanction in the event of legal involvement of the company), indirect losses (cost of the measures necessary for the restoration of *business as usual* operations) and consequential damage (damage to image or reputation with potential repercussions on losses of market share);
- the analysis of cases that have occurred in other companies (*fraud business cases*) and which have become known through the media.

The Function Managers shall contribute to an effective analysis and assessment of risk through open and loyal collaboration with the Chairman/Single Member of the SB and the HIA, providing the necessary data and information and their more in-depth knowledge of business processes.

8. WHISTLEBLOWING NOTIFICATIONS

Whistleblowing is understood as meaning the possibility of notifying cases of any offenses falling within the scope of the European Union or national acts indicated in the annex to Legislative Decree No. 24/2023, of relevant illegal conduct pursuant to Legislative Decree 231/2001 or suspected frauds and/or infringements of the Code of Ethics and of the Organisational Model, of which the Recipients of this *policy* have become aware for business reasons, with the guarantee of absolute protection of the identity of the whistleblower, with the aim of avoiding any form of discrimination against the same party.

In addition, the following situations may be notified:

- acts or omissions that harm the financial interests of the European Union or of the internal market;
- acts or conduct that defeat the object or purpose of the provisions of the acts of the European Union in the aforementioned areas.

In any case, it is the primary duty of the body managing the notification, composed of the Chairman/Single Member of the Supervisory Body and of the HIA to adopt any measure aimed at ensuring the confidentiality of the identity of the notifying person, of the facilitator, of the involved person or, in any case, of the subjects mentioned in the notification and the content of the notification and its documentation.

In particular, the entities comprising the managing body:

- receive a formal assignment as members of the managing entity of the internal channels, which also includes the letter of designation as authorised pursuant to Arts. 29 of EU Reg. 679/2016 (also, the "GDPR") and 2-*quaterdecies* of Legislative Decree No. 196/2003 (also, the "Privacy Code"). The letter provides specific instructions for the correct processing of personal data described in the notification, of which the Companies are Data Controllers pursuant to Art. 4, para. 1, item 7) of the GDPR.
- ensure independence and impartiality;
- receive adequate professional training in the discipline of whistleblowing, also with reference to concrete cases.

If the internal notification is presented to a subject other than the identified and authorised one, the notification shall be forwarded, within seven days of its receipt, to the competent subject, giving simultaneous notice of the forwarding to the notifying person.

It should be noted that Presidential Decree No. 62 of 2013 provides that the notification may be submitted to the hierarchical superior, but that this notification may not be considered as whistleblowing and hence that the whistleblower will not be able to benefit from the protection provided by Legislative Decree No. 24/2023.

To this end, the company provides the following channels for receiving the notification:

- *Whistleblowing* platform, which permits the forwarding of written notifications, accessible from any browser (including with access from mobile devices), with the following address **https://esprinet.eticainsieme.it**. This instrument offers the broadest guarantees of confidentiality for the whistleblower;

- calling the telephone number **+393427755190** (not subject to the registration procedure) managed by the HIA, which acknowledges the request, proposing the setting of an appointment and, in cases of particular urgency, receiving the notification at the same time. A summary report shall be drawn up of this conversation, which is brought to the attention, in observance of the confidentiality of the whistleblower, of the other member of the body managing the notification (Chairman/Single member of the SB) and, within seven days of the call/message, the latter party shall forward it to the whistleblower, by e-mail to the address notified by the latter party, so that the same whistleblower can verify, rectify, confirm its content and sign it. After confirming the content, the HIA may register the notification within a specific section of the Whistleblowing platform, including the e-mail reference provided by the whistleblower, in order to allow the automatic forwarding of a unique code, necessary for monitoring the progress of the processing of the same.

After sending the notification, through the Platform or by phone call, it is then possible to book a meeting to be held in person.

8.1. CONTENT OF THE NOTIFICATION

The whistleblower is obliged to provide all the elements known to him or her which are useful for checking the reported facts, with the due verifications. In particular, the notification shall be detailed and complete in order to allow the assessment of the notified fact and shall contain the following essential elements:

- the personal details of the person making the notification, indicating any role within the company or entity where his or her work is carried out, as well as the consent, or absence of it, to use he identity of the same, immediately or subsequently, in the verification activities and therefore reveal the identity of the same to parties other than the managers of the notification and/or to the office of the staff responsible for managing the disciplinary procedure;
- a clear and complete description of the actions forming the object of the notification;
- the circumstances of time and place in which the notified actions were committed;
- the details of the person who carried out the actions forming the object of the notification;
- the indication of the beneficiaries and those harmed by the offence or infringement;
- the indication of any other persons who may report on the facts forming the object of the notification;
- the attachment of any documents that may confirm the well-foundedness of the reported facts;
- any other information that may provide useful feedback on the existence of the notified facts.

The notification also provides for the need for the whistleblower to declare his commitment to report what he knows to be true.

8.2. NOTIFICATION PLATFORM

The notification platform adopted, resident on the server of a third party, provides for a confidential registration, the use of encryption and a guided route for the whistleblower that will allow the same party to enter the necessary information listed in paragraph 8.1.

The Italian Esprinet Group companies have adopted a single notification platform (eticainsieme) that allows the whistleblower to indicate the Companies to which the notification refers; indeed, on the home page, a screen is displayed that shows an indication of all of the Companies. It should be noted that organisational and security measures are adopted that allow each Company to access the notifications for which it is responsible.

The platform provider has signed the data protection agreement pursuant to Art. 28 of the GDPR, with which it undertakes to comply with the instructions provided by the Data Controller Companies, including in the event of subcontracting.

The whistleblower shall complete a series of open and closed questions, which will allow the recipient of the notification to investigate the subject of the same at first sight, even without creating a direct contact with the whistleblower.

At the end of the notification procedure, the platform will provide the whistleblower with a code which permits the same party to access the system and hence his or her own notification, in order to:

- monitor its progress;

- supplement his or her notification with additional factual elements or other documentation;
- have direct contact with the recipients of the notification, also initiating a possible exchange of requests and information.

The platform also permits the uploading of the documentation that the whistleblower considers appropriate to bring to the attention of the channel managers in support of his or her notification.

8.3. MANAGEMENT OF REPORTS

Once the notification has been received, the managing body of the same, after having given evidence to the notifying party of the assumption within the seven-day deadline, will analyse it, with the possibility of involving the other figures and functions identified in the previous paragraphs on the basis of a preliminary assessment of the seriousness of the subject of the notification and of the possible subjects and functions involved in the notified events.

As part of the investigation, the managers of the notification:

- maintain discussions with the notifying party and may request additional information from the notifying party, if necessary. Through the use of the platform, it is possible to exchange requests between the whistleblower and the recipient of the notification in order to deepen the topics forming the object of the notification.
- carry out the appropriate checks, if necessary, involving third parties (internal or external to the Companies) who have the necessary skills to manage the notification received;
- hear the involved person, also at his or her request, orally or through document-based proceedings, through the acquisition of written observations and documents.

In any case, the personal data of the whistleblower and any other information from which this identity may be derived directly or indirectly, shall not be disclosed to third parties by the recipients of the notifications without the consent of the whistleblower, in order to protect him or her from possible retaliation or discrimination. It should be noted that, even in the absence of consent but which becomes necessary for investigative reasons, if other subjects must also be made aware of the content of the notification and/or the documentation attached to it, the managers will ensure that the personal data of the Whistleblower is obscured, as well as that of the other subjects whose identity must remain confidential (the facilitator, the notified party, the other persons mentioned in the notification).

Through the use of the platform, it is possible to exchange requests between the whistleblower and the recipient of the notification in order to deepen the topics covered by the communication or to organize the meeting scheduled for the management of the oral channel.

The appropriate checks shall be carried out, including any hearing of the whistleblower, if he or she gives his or her consent or requests it, and, in the event that the notification is well-founded, the competent company functions shall be informed so that the appropriate disciplinary actions are taken, also involving the Company's

management and control bodies.

Within 3 months of receiving the notification, the recipients of the notification shall diligently follow up on the notification and provide feedback.

At any time after receiving the notification, the recipients may archive it if they consider it irrelevant by way of this procedure.

At the end of the investigation, the recipients shall draw up a notification taking one or more of the following measures:

- archiving of the notification due to irrelevance;
- proposal to amend the Organisation, Management and Control Model and/or the Code of Ethics;
- proposal to initiate disciplinary or sanctioning proceedings, in accordance with the provisions of the Organisation, Management and Control Model, against the subjects notified and whose committing of an offence or infringement has been recognised;
- proposal to initiate disciplinary or sanctioning proceedings, in accordance with the provisions of the Organization, Management and Control Model and this procedure, against whistleblowers who have made unfounded notifications, based on factual circumstances that are not true and are carried out with malicious intent or gross negligence.

8.4. REPORTING THROUGH EXTERNAL CHANNELS

In accordance with current legislation, the whistleblower may make an external notification, to be submitted to ANAC, if:

- it has already made an internal notification that has not been followed up;
- there are well-founded reasons for believing that, if it made an internal notification, it would not be effectively followed up or could become the object of retaliation;
- it has reasonable grounds for believing that the breach may constitute an imminent or manifest danger to the public interest.

The notification procedures are defined by ANAC and published on its website, at https://www.anticorruzione.it/-/whistleblowing.

In the event of retaliations committed in the work context of a private sector subject, the ANAC shall inform the National Labour Inspectorate, for the measures within its competence.

8.5. PUBLIC DISCLOSURE

Lastly, the whistleblower has scope for making the notification through public disclosure, benefiting from the protection provided by this policy, only if:

- it has previously made an internal or external notification without having received feedback within the established deadlines;
- it has reasonable grounds for believing that the breach may constitute an imminent or obvious danger to the public interest;
- it has reasonable grounds for believing that the external notification may involve the risk of retaliation

or may not have an effective follow-up due to the specific circumstances of the actual case, such as those in which evidence may be concealed or destroyed or in which there is a well-founded fear that the person who received the notification may be in collusion with the perpetrator of the infringement or involved in the infringement itself.

8.6. FILING

The Platform used by the Company permits the storage of notifications and attached documentation in computer and encrypted mode as well as in accordance with the applicable legislation on the protection of personal data.

Any other documentation produced by the recipients of the notifications shall be archived and kept in observance of confidentiality for a maximum deadline of five years, except for any requests from the Authority (e.g. the establishment of criminal proceedings).

8.7. INFORMATION ON THE PROCESSING OF DATA DERIVED FROM THE MANAGEMENT OF NOTIFICATIONS

In accordance with current data protection legislation, we inform data subjects that their personal data will be processed by the Italian Esprinet Group company which receives the notification, the Data Controller, for the sole purpose of processing this notification.

The following are considered to be interested parties:

- the notifying person: the natural person who makes the notification on infringements acquired within their work context;
- the facilitator: a natural person who assists a notifying person in the notification process, operating within the same working context and whose assistance must be kept confidential;
- the person involved: the natural person mentioned in the notification as the person to whom the infringement is attributed or as the person in any case involved in the notified infringement.

The Data Controller shall process the personal data of the data subjects described below:

- identification and contact data, such as first name and surname, e-mail address or telephone number;
- data relating to the relationship with the Data Controller;
- other data which shall be entered by the notifying person in the compilation of the notification form/provided over the phone or subsequently acquired by the managers of the notifications as part of the investigative activity.

The personal data and other information provided may be brought to the attention of the figures and offices identified in the previous paragraphs for the correct investigation and processing of the notification.

The legal basis for the processing indicated above can be found in the fulfilment of the legal obligation pursuant to Art. 6, para. 1, item c) of the GDPR, as described in Legislative Decree No. 24/2023.

The legal basis can also be found, with regard to the processing of particular categories of data, in Art. 9, para. 2, item b) of the GDPR as the processing is necessary for fulfilling the obligations and exercising the specific rights of the data controller or data subject in the field of labour law and social security and social protection, as well as in Art. 9, para. 2, item g) of the GDPR, insofar as the processing is necessary for reasons of relevant public interest on the basis of Art. 2-*sexies* of Legislative Decree No. 196/2003.

The processing of judicial data that may be necessary for the management of *whistleblowing* notifications received is legitimate on the basis of Art. 10 of the GDPR, in correlation with Art. 2-*octies* of Legislative Decree No. 196/2003

Data quality

Whistleblowers must have reasonable grounds for considering that the personal data and information on breaches contained in the notification is true, accurate and up-to-date.

The personal data provided in the context of the notifications shall thus be processed in accordance with the applicable legislation on the protection of personal data and for the legitimate purposes relating to the investigations deriving from the notification, they cannot be used for purposes incompatible with this purpose, they must be adequate and not excessive for these purposes.

In particular, the Data Controller shall process the personal data of the data subjects solely for the following purposes:

- assumption of the notification by the managers,
- sending of any requests and/or receiving feedback on requests sent by the whistleblower and the managers of the notification,
- investigative management: carrying out checks on the validity of the notification,
- management of the resulting measures, also from a disciplinary perspective.

Rights of access, rectification, cancellation, objection, restriction of data processing or withdrawal of consent

Each of the companies comprising the Esprinet Group shall be regarded as the Data Controller for complaints submitted in accordance with the procedure regulated in this Policy when complaints concern its staff.

The rights described in Arts. 15 to 22 of Regulation (EU) 2016/679 (the right of access to personal data, the right to rectify these, the right to obtain their erasure or so-called right to be forgotten, the right to restriction of processing, the right to portability of personal data and the right to object to processing) may be exercised within the limits of the provisions of Art. 2-*undecies* of Legislative Decree No. 196/2003, i.e. they may be limited if the request may result in an actual and concrete prejudice, for example, to the confidentiality of the identity of the whistleblower or to the conduct of defensive investigations or to the exercise of a right in court. To exercise such rights, data subjects may send an e-mail to dpo@esprinet.com, indicating the specific right that they wish to exercise.

Notification and data transfer

In addition, the data relating to thenotifications may be notified to the other Group companies, whose names and addresses appear on the www.esprinet.com website when the internal body responsible for the notification considers that their intervention is necessary for the investigation and clarification of the facts.

In addition, data received through the internal notification system described in this Policy may be disclosed to other entities that provide consultancy services necessary for the correct management of notifications, these will act as data processors.

Document retention and retention period

The data processed as part of the investigations shall be retained for a period of time not exceeding five years from the end of the investigation relating to the notification, unless the Data Controller has documented the need to keep the data for a period of more than five years, for example in the event of disciplinary, administrative or judicial proceedings.

Measures shall be adopted to ensure adequate security and confidentiality of the information, with the possibility of establishing enhanced security measures and taking extreme precautions to ensure compliance with the duty of confidentiality, taking into account the nature of the collected data.

It is understood that personal data that are manifestly not useful for the processing of a specific notification shall not be collected or, if accidentally collected, shall be deleted immediately.

9. OTHER DETECTION SYSTEMS

9.1. NOTIFICATIONS TO THE SUPERVISORY BODY

The Supervisory Body, in addition to ordinary information flows, is required to receive notifications relating to alleged infringements of the Organisational Model that may constitute a direct or indirect "231" risk.

Such information is necessary to allow the Body to take timely action to prevent the committing of the offences provided by Legislative Decree No. 231/2001 and to ensure compliance with the rules that form an integral part of the Model itself.

9.2. ORDINARY AUDIT ACTIVITIES

The Internal Audit, during the ordinary checks provided by the Audit Plan, may detect symptomatic signs of fraudulent behaviour or serious infringements of the Code of Ethics (the so-called red flag).

In these cases as well, once a preliminary evaluation has been carried out, it shall proceed as established in Chapter 13.

9.3. CUSTOMER COMPLAINTS

In addition to requiring prompt intervention for reasons of customer satisfaction, customer complaints may involve fraudulent aspects or conduct which may be contrary in some way to the Code of Ethics.

For this reason, anyone who receives such complaints shall assess them carefully and only inform the Supervisory Body in the most serious cases.

10. PROTECTION OF WHISTLEBLOWERS

Except in cases where criminal liability may be characterised by way of slander or defamation pursuant to the provisions of Art. 2043 of the Italian Civil Code, the identity of the whistleblower shall be protected at every stage following the notification itself.

In this way, the identity of the whistleblower may not be revealed without their express consent and all those who receive or are involved in handling notifications shall be required to protect their confidentiality.

Infringement of the obligation of confidentiality shall represent a serious disciplinary infringement.

In the same way, any form of retaliation or discrimination implemented against the notifying party shall represent a serious disciplinary infringement, with this party required to report such behaviour to his or her direct hierarchical superior or directly to the SB. Forms of retaliation or discrimination shall include the following, by way of example:

a) dismissal, suspension or equivalent measures;
b) demotion or non-promotion;
c) change in duties, change of workplace, reduction in salary, change in working hours;
d) suspension of training or any restriction of access to it;
e) negative credit ratings or negative references;
f) adoption of disciplinary measures or of other sanctions, including financial penalties;
g) coercion, intimidation, harassment or ostracism;
h) discrimination or unfavourable treatment in any way;
i) failure to convert a fixed-term employment contract into a permanent employment contract, where the worker had a legitimate expectation of the said conversion;
j) non-renewal or early termination of a fixed-term employment contract;
k) damage, including to the person's reputation, in particular on social media, or economic or financial losses, including loss of economic opportunities and loss of income;
l) placing on inappropriate lists on the basis of a formal or informal sectoral or industrial agreement, which may make it impossible for the person to find employment in the sector or industry in the future;
m) the advance conclusion or cancellation of the contract for the supply of goods or services;
n) the cancellation of a licence or permit;
o) a request to submit to psychiatric or medical investigations;
p) demanding results that are impossible to achieve in the indicated manner and within the indicated time;
q) an artificially negative performance assessment;
r) unjustified revocation of assignments; unjustified failure to confer assignments with simultaneous attribution to another person;
s) repeated rejection of requests (e.g. holidays, leave);
t) unjustified suspension of patents, licenses, etc.

In any case, the retaliatory or discriminatory dismissal of the person who notifies the facts falling within the Whistleblowing issue shall be null and void. The change of duties pursuant to Art. 2103 of the Italian Civil Code

shall likewise be null and void.

Lastly, in the event of disputes arising from the imposing of disciplinary sanctions or demotion, dismissal, transfer or subjection of the informant to another organisational measure with direct or indirect negative effects on his/her working conditions, the Employer shall be required to demonstrate that such measures are in no way a consequence of the notification itself.

The protection of the whistleblower shall also be extended in the case of anonymous notification, which is then followed by the identification of the whistleblower. In addition, anonymous notifications received shall be regarded as ordinary notifications to be treated according to the criteria established in this policy and in local legislation.

It is also specified that protection for the whistleblower is not guaranteed in cases of:

- a first instance ruling for defamation and slander;
- cases of misconduct or gross negligence.

The identity of the whistleblower, by written communication of the reasons for the disclosure of confidential data , may only be revealed to the Human Resources function and to the accused in the following cases:

- when the whistleblower has given his or her express consent;
- in disciplinary proceedings, when the disciplinary challenge is found to be based, as a whole or in part, on the notification and knowledge of the identity of the notifying party is absolutely essential to the defence of the accused party. In any event, the verification activity shall aim to acquire independent evidence that does not require recourse to this latter requirement.

10.1. UNACCEPTABLE NOTIFICATIONS

The notifications shall always have a content from which a loyal spirit of participation in the control emerges. The following are also prohibited:

- the use of insulting expressions;
- the forwarding of notifications for purely defamatory or slanderous purposes;
- the forwarding of notifications that relate exclusively to aspects of private life, without any direct or indirect connection with the company's activity. These notifications shall be considered even more serious when they refer to sexual, religious and political habits and orientations;
- the forwarding of claims, disputes, requests of a personal nature of the notifying person or of the person who has filed a complaint with the judicial or accounting authority, relating exclusively to their individual employment relationships, or inherent to their employment relationships with hierarchically superior figures;
- to notifications of infringements, where they are already mandatorily governed by the acts of the European Union or national acts indicated in part II of the annex to this decree or by national acts that constitute the implementation of the acts of the European Union indicated in part II of the annex to Directive (EU) 2019/1937, even if not indicated in part II of the annex to this decree;

- to notifications of national security breaches, as well as of procurement relating to defence or national security aspects, unless such aspects fall within the relevant secondary law of the European Union.

11. PERMITTED AND PROHIBITED CHECKS

11.1. INDIRECT CONTROLS

Any indirect control over the activity of workers carried out through work tools (e-mails, badges, PCs, mobile phones, etc.), made necessary for organisational reasons, safety in the workplace and protection of company assets, may also be used for the purpose of ascertaining alleged fraudulent behaviour or behaviour contrary to the Code of Ethics (e.g. unauthorised use of the access credentials of others).

To this end, adequate information is given to the individual worker in advance about the methods of use of these tools, as well as about the methods of carrying out checks.

In any case, the privacy principles of proportionality, relevance and non-excess must be respected.

Controls with a vexatious character shall always be prohibited.

11.2. CONTROLS USING VIDEO SURVEILLANCE SYSTEMS

Controls by means of audiovisual systems and other instruments from which the possibility of remote control of workers' activity also derives can be carried out exclusively for organisational and production needs, for job safety and for the protection of company assets.

In case of installation of the audiovisual systems, adequate information shall be given to the individual worker in advance about the methods of use of these instruments, as well as about the methods of conducting the controls.

11.3. DIRECT CONTROLS

Direct control means any intervention by the direct superior or the control functions with regard to the employee. This is not only permitted, but is mandatory.

This form of control represents the expression of the duty-management power of those who have a responsibility for the achievement of corporate objectives and for compliance with the rules.

Direct control must aim at the dissemination of virtuous conduct and respect for the Code of Ethics and company procedures.

In the event of suspected fraudulent behaviour or behaviour contrary to the Code of Ethics, the direct manager and staff of the Internal Audit function may assume:

- control of the workstation;
- direct control over the content of the company PC provided to the individual employee.

These checks shall always take place exclusively in the presence of the directly concerned person and only in exceptional, urgent and serious cases will the check be allowed even in his or her absence, but in the presence of a colleague indicated by him or her or of a trade union representative.

12. IT SECURITY POLICIES

All employees shall be required to comply with the provisions of *LIG01001 Company policy on the use of IT tools and information security*.

The provisions of para. 11 of this policy regarding the usability of the results of the monitoring required for reasons of verification of any illegal conduct shall apply.

We also recall the provisions of the aforementioned Policy.

13. PROCEDURES FOR CARRYING OUT AND DOCUMENTING INTERVIEWS

During an audit conducted by the HIA and/or by the President/Single member of the SB, aimed at ascertaining the veracity of the subject of the notification, interviews may be conducted of employees and/or staff members able to report useful circumstances.

Anyone, summoned to a hearing by the HIA and/or by the President/Single member of the SB, shall be obliged:

- to introduce him/herself;
- to cooperate loyally and with the greatest transparency, reporting any circumstances known to him or her in relation to the facts and questions asked of him/her;
- to provide any additional documentation requested, in support of the provided information;
- to sign the interview report that will be drawn up.

the HIA and/or the Chairman/Single member of the SB shall take care:

- to avoid the assumption of harassing or inquisitive attitudes towards the interviewed employee/staff member, even when the latter party is the alleged perpetrator of the infringement:
- not to allow anyone other than the interviewee to attend the hearing;
- not to issue a copy of the interview report;

The interview shall in no way constitute a disciplinary challenge, even when it concerns the alleged perpetrator of the infringement forming the object of the investigation.

14. METHODS AND CRITERIA FOR TRACEABILITY, ARCHIVING, CONTROL AND REPORTING OF ACTIVITIES CARRIED OUT

The verification activities shall comply with the general principles of the SCIGR and the professional standards of the auditors, also in terms of traceability, archiving and reporting of verification activities.

Given the particular nature, however, of the data collected during a verification activity, also for privacy purposes this documentation shall be subject to reinforced security measures.

It is prohibited for anyone to delete or destroy e-mails, files or documents to be retained by way of execution of a legal obligation, for tax reasons and for express provisions of company policies. In addition, any electronic

document (e-mail, file, etc.) attributable to operations which depart from company policies shall be tracked and stored.

15. MANAGEMENT OF ANY RELATIONS WITH THE POLICE AND JUDICIAL AUTHORITIES

In the event that it becomes necessary, for serious events, to request the intervention of the Law Enforcement Forces, the Supervisory Body shall inform the Security Manager, who shall take action according to territorial and functional competences. Any complaints/claims shall be processed and filed by the Legal Department.

Anyone summoned by the Judicial Police or by the Judicial Authority or by the Criminal Judge, as a person informed of the facts or as a witness to events relating to the activity of the company or to ascertained fraud or illegal action for which a complaint/complaint has been filed by the company, shall be required to inform the Supervisory Body, which may authorise the viewing of internal records or statements previously made during the interview, as a memory aid and to allow effective and transparent collaboration with the Police and Judicial Authorities.

Other than these cases, the summoned person shall maintain absolute confidentiality regarding the details and reasons for the summons received.

16. SYSTEM OF SANCTIONS

The system of sanctions applied within the company and stipulated by the CCNL provides for the imposing of the following disciplinary sanctions:

- verbally attributed blame for minor faults;
- guilt attributed in writing in cases of repeat offences of the type cited in the preceding point;
- a fine not exceeding the amount of 4 hours of normal remuneration;
- suspension from pay and service for a maximum of 10 days;
- disciplinary dismissal without notice, with the other consequences of reason and law.

The choice of the penalty to be paid shall be commensurate, according to the principle of gradualness, following the verification of the seriousness of the offence committed, notably considering:

- evidence collected in the disciplinary proceedings;
- the voluntary or culpable nature of the infringement committed;
- the repeated nature of the illegal conduct;
- the damage, even potential, caused to the company, understood both as a physical structure and as a population of employees/staff.

With specific reference to the regulation of *whistleblowing notifications* described in this *policy*, while not constituting an exhaustive list, the following infractions are always a source of disciplinary responsibility:

a. with regard to all subjects who:
   - hinder or attempt to hinder the notifications described in this policy;
   - infringe the obligation of confidentiality of the identity of the whistleblower and any other information referred to in the notifications indicated above;
   - implement forms of retaliation or discrimination against the whistleblower and facilitators;

b. with regard to all subjects who have adopted this policy:
    - when it is found that it does not comply with the provisions of Arts. 4 and 5 of Legislative Decree 24/2023;

c. with regard to those parties who investigate the notifications:
    - when the verification and analysis of the reports received has not been carried out;

d. with regard to whistleblowers:
    - in the event that the criminal liability of the whistleblower is ascertained, even with a decision by the court of first instance, for the crime of defamation committed with the notification or for the crimes of slander or defamation committed with the denunciation to the judicial or accounting authority or if the civil liability of the whistleblower is ascertained for conduct attributable to the crimes indicated above in the event of wilful misconduct or gross negligence;

e. against the involved person who has been guilty of significant infringements/offences under this policy, in the event that the notification has proven to be well-founded.

Finally, any other infringement of the procedural rules set out in this policy shall constitute a disciplinary offence.

17. FILING

The original paper copy of this policy is filed at the Internal Audit office, as evidence of the signatures for drafting, checking and approval.

A copy has been filed in the company document system.