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

Company:
Esprinet Ibérica, V-Valley Advanced Solutions España, Esprinet Portugal

Facility:
All facilities

Subsystem:
Regulation 2016/679, Penal Code

File name
ESDIS01001 Policy for the prevention of fraud and violations 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	Whistleblowing update	P. Aglianò CRO	G. Monina RIA	A.Cattani AD
01	15/10/18	Whistleblowing update	P. Aglianò CRO	G. Monina RIA	A.Cattani AD
02	29/06/21	Update	P. Aglianò CRO	G. Monina RIA	A.Cattani AD
03	16/03/22	Extension to V-Valley Advanced Solutions España	P. Aglianò CRO	G. Monina RIA	A.Cattani AD
04	08/06/22	Extension to Dacom S.p.A.	P. Aglianò CRO	G. Monina RIA	A.Cattani AD
05	13/11/23	Portuguese regulations and Law 02/2023 update	A. Biffi Risk Manager	G. Monina RIA	A.Cattani AD

CONTENTS

1. PURPOSE AND SCOPE

This policy summarises the principles established by the Company for the purpose of effectively managing the reporting of fraudulent and illegitimate behaviour and, in any case, behaviour contrary to the Code of Ethics and the Organisational Model of the Companies and to any applicable regulations in effect, by all employees (hereinafter referred to as the Esprinet Group) and collaborators of the Esprinet Group.

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 various Criminal Codes 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 different Criminal Codes;
- 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 Esprinet Group employees, collaborators [1] and customers and to the part relating to the notification of Whistleblowing breaches by all Recipients of the Code of Ethics and of the Organisational Model.

It shall also be the responsibility and duty of each head of department to disseminate the principles to suppliers, consultants and occasional collaborators.

[1] collaborators are understood as including employees of suppliers, collaborators on projects, agents and any person working on a permanent basis with the Esprinet Group.

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.
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).
IRREGULAR BUSINESS CONDUCT	Any event of a human nature (conduct or subjective element) that causes or may cause a loss to the company.
NORMATIVE INFRINGEMENT	Is understood as meaning the committing or possible committing of an offence for which entities are liable pursuant to the Spanish Penal Code (Organic Law 10/1995 of 23 November) and the Portuguese Penal Code (Decree-Law No. 48/95). These offences are listed in the various Penal Codes and in all other applicable legislation.

IRREGULARITY	These are considered to be breaches of the procedures and rules provided in the Code of Ethics and/or in the Organisational, Management and Control Model of Esprinet Group companies.
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).
RED FLAG	Relevant indicators of potential fraud or abuse, constituting grounds for initiating an audit.
WHISTLEBLOWING or the INTERNAL INFORMATION SYSTEM	A reporting system through which a stakeholder who, while carrying out his or her work activity or maintaining a business relationship with the Esprinet Group, detects a potential fraud, tort, regulatory infringement, irregularity, danger or other serious risk carried out by an employee of the Esprinet Group and/or a collaborator, that may harm customers, colleagues, shareholders, the public or the integrity and reputation of the company/public entity/foundation and decides to report it to the Esprinet Group.
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
HIA	Head of Internal Audit
CdS	Collegio Sindicale
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.

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	Spanish Penal Code (Organic Law 10/1995, of 23 November)
	Portuguese Penal Code (Decree-Law No. 48/95)
	Law No. 34/87 of 16 July
	Law No. 20/2008 of 21 April
	Law 2/2023 of 20 February, on the protection of persons who report regulatory infringements and on combating of corruption.
	Organic Law 3/2018, of 5 December, on the Protection of Personal Data and the guarantee of Digital Rights.
	Law No. 58/2019 of 8 August (Personal Data Protection Act)
	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).
	Royal Legislative Decree 2/2015, of 23 October, approving the revised text of the Workers' Statute Law
INTERNAL PROCEDURES AND DOCUMENTS	Code of Ethics
	Internal disciplinary system
	Organisation, management and control model adopted for Spain and Portugal
	Internal Regulations for the Use of IT Tools
	Procedure for Giveaways of Goods
	Anti-Corruption Policy
	Conflict of Interest Policy of the Esprinet Group in Spain
	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 disciplinary system

6. ROLES AND RESPONSIBILITIES

6.1. Chief executive officers

The Chief Executive Officers (or the corresponding functions in the various companies of the Group Esprinet) 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.
- these assume responsibility for implementing an Internal Information System in the Esprinet Group in Spain, appointing the person in charge of the Information System within the Esprinet Group in Spain and adopting the information management procedure.

6.2. The Supervisory Bodies of the Esprinet Group in Spain as Responsible for the Internal Information System

The Corporate Supervisory Body of each of the Esprinet Group companies in Spain has been designated as the Body Responsible for the Internal Information System, being organised on a collegiate basis, with its members recognised as having sufficient competence to manage the notifications reported through the authorised channels. In this regard, the body designated as responsible for the Internal Information System shall perform its duties, guaranteeing the absence of conflicts of interest, as well as in an independent and autonomous manner with regard to the other bodies of the Company, including the Board of Directors. The main function of the Internal Information System Manager shall be the diligent management of the information management procedure implemented by the Esprinet Group in Spain.

6.3. 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).

6.4. 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 regard to cases of notification of Whistleblowing breaches, the Esprinet S.p.A. Supervisory Body shall be informed by the Spanish or Portuguese Supervisory Body in the most serious cases involving senior management, members of the Supervisory Body or other members of the Supervisory Body or which, in any case, could have a serious impact or affect the correct management of the company.

6.5. Internal Audit

Internal Audit:

- 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.

6.6. Human Resources

The Head of Human Resources:

- It shall be informed of the facts reported by the whistleblower and shall only intervene in support of the Supervisory Body when disciplinary measures may be taken against an employee or when it intervenes as an investigator in the investigation process. 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.

6.7. Legal department

The in-house Lawyer:

- It may be informed of the facts reported by the whistleblower and may intervene in support of the Supervisory Authority, assessing the criminal nature of the alleged facts and verifying, with the help of external lawyers, whether the offence is punishable *ex officio* or on the basis of a complaint by one of the parties.

6.8. 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
- to maintain the confidentiality of the identity of the employee or whoever informs him or her of any of the facts cited in the preceding point;
- To avoid discriminatory or vexatious behaviour and, in general, reprisals against those parties who notify the facts mentioned in the previous 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. ASSESSMENT OF THE RISK OF FRAUD AND OF CONDUCT CONTRARY TO THE CODE OF ETHICS

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.

7.1. Internal information channels

The detection of potential cases of fraud may benefit from the loyal contribution of all employees and recipients of this policy.

All employees of the Esprinet Group are obliged to report, through the channels indicated in the following section and provided by the Company, any fraud, infringement or breach of the Code of Ethics and the Organisational Model and breaches of regulations that have occurred or are merely suspected.

7.2. Whistleblowing

Whistleblowing means the possibility of notifying cases of possible offences, breaches of regulations, suspected fraud and/or infringements of the Code of Ethics and the Organisational Model, of which employees and collaborators have become aware for work-related reasons, with the guarantee of absolute protection of the whistleblower's identity, with the aim of avoiding any kind of discrimination against this party.

In each case, it is the primary duty of employees and/or collaborators to inform the competent Supervisory Authority and for this latter entity to take all measures to ensure the confidentiality of the identity of the whistleblower.

To this end, the company shall provide the following reporting channels:

- by letter to the SURVEILLANCE BODY as a function of the country of the Company to which the complaint is transferred:
    - Spain:
        - Esprinet Ibérica. Calle Osca 2 -Campus 3-84 - Pol. PLAZA (Plataforma Logística de Zaragoza), 50197, Zaragoza, Spain
        - V-Valley Advanced Solutions España, S.A.U. Calle Osca 2 -Campus 3-84 - Pol. PLAZA (Plataforma Logística de Zaragoza), 50197, Zaragoza, Spain
    - Portugal:
        - AVIZ Trade-Center Building Rua Eng. Ferreira Dias, 924, 1º - Escritório E19 4100-246, Porto, Portugal
- *Whistleblowing* platform accessible from any browser (including mobile devices) at https://esprinet.eticainsieme.it. The latter instrument offers the broadest guarantees of confidentiality for the whistleblower and the possibility of anonymous notifications.
- E-mail sent to the Supervisory Authority from:
    - Esprinet Ibérica, SLU: odveib@esprinet.com

- V-Valley Advanced Solutions España, SAU: odv@v-valley.es
- Esprinet Portugal, LdA: odvep@esprinet.com

- Through a face-to-face meeting between the whistleblower and members of the Competition Monitoring Authority. Such a meeting shall be held within seven (7) days of the whistleblower's request.

  The face-to-face meeting must be documented, subject to the whistleblower's consent, by means of:
  - Recording of the conversation in a secure, durable and accessible format, providing information regarding data protection rights; or
  - Complete and accurate transcription of the conversation, allowing for verification, rectification and acceptance by signature of the whistleblower.

  In the event that the whistleblower does not provide such consent, the Supervisory Authority shall keep a record of the meeting held.

In addition, persons who become aware of information that may involve the committing of a regulatory infringement or an offence may also report the facts forming the object of the notification through the channels provided by the competent national public authorities or, failing this, by the competent authorities of the autonomous communities that have designated a body for this purpose.

The Esprinet Group in Spain and Portugal has adopted a procedure for managing the reporting of regulatory breaches.

7.3. 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 details of the person making the offence report, indicating his or her current or former role in the company, except where the whistleblower chooses to make the report anonymously. The whistleblower has the right to make the notification anonymously;
- 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 infringement;
- the attachment of any documents that may confirm the well-foundedness of the reported facts;
- any other information that may provide useful information on the existence of the reported facts.

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

7.4. Platform for notification of infringements

The adopted notification platform, hosted on the server of a third party, provides for confidential registration, the use of encryption techniques and a guided path for the whistleblower to enter the necessary information listed in Section 8.2. In this way, the platform also allows for anonymous notifications.

The whistleblower is asked to fill in a series of open and closed questions, allowing the recipient of the notification to go deeper into the subject of the notification in the first instance, even without creating a direct contact with the whistleblower himself/herself.

At the end of the reporting process, the platform will acknowledge receipt of the same and shall provide the whistleblower with a code that will allow him/her to access the system and hence, to make his/her notification for:

- monitoring the progress of the project;
- integrating his/her knowledge with additional factual elements or other documentation;
- making direct contact with the recipients of the notification, also initiating possible exchanges of requests and information.

7.5. Management of notification of infringements

The recipient shall notify the whistleblower of the receipt of the notification within at most 7 days of its receipt, and shall analyse it within 15 days, with the possibility of involving the other figures and departments identified in the previous paragraphs on the basis of a preliminary assessment of the seriousness of the subject of the report and of the possible subjects and departments involved in the reported facts.

Through the use of the platform, there is the possibility of exchanging requests between the whistleblower and the recipients of the offence in order to deepen the topics of notification.

Appropriate checks shall be carried out, including possible hearings with the whistleblower if he/she gives his/her consent. In the event that the notification of a breach proves to be well-founded, the corporate departments of the company shall be informed and the disciplinary actions taken which involve the management and control bodies of the Company.

Within at most 90 days (3 months) of the notification from the reporting party, the competent body shall complete the preliminary investigation and inform the reporting party of the outcome. Additionally and for cases of special complexity, the period may be extended for up to another three (3) months, for a total of six (6) months, and the Supervisory Body shall provide reasons justifying such a temporary extension.

At any time after receiving the notification, recipients may archive it if they consider it irrelevant under this Policy.

At the end of the investigation, the recipients shall write a report taking one or more of the following actions:

- archiving of the notification on grounds of irrelevance;
- a proposal to modify the Organisation, Management and Control Model, internal policies and

procedures and/or the Code of Ethics;

- a proposal to initiate disciplinary or sanctioning proceedings, in accordance with the provisions of the Organisation, Management and Control Model, in relation to the reported facts and for which the committing of an offence or irregularity 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.

7.6. Recording of information

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.

This register shall be managed in computerised and encrypted form and in accordance with the applicable legislation on the protection of personal data. It should also be noted that the register will not be made public and will be accessible only to the competent judicial authority that submits a reasoned request through an order issued in the context of legal proceedings.

Any other documentation produced by the recipients of the notifications will be archived and kept confidential.

8. PERSONAL DATA PROTECTION AND ACCESS TO DATA

The Esprinet Group undertakes to comply with data protection regulations and to adopt the necessary organisational and technical measures for guaranteeing the confidentiality, integrity and availability of the data processed within the context of the process of managing the reporting of infringements.

In any event, access to the personal data contained in the file and/or the facts that are the subject of the notification shall be limited to the following persons:

- The competent Supervisory Authority and whoever manages it directly;
- The Human Resources Manager, only when disciplinary measures may be taken against an employee. In the case of public sector employees, the body responsible for its processing;
- The person in charge of the legal services of the entity, if any legal action should be taken in relation to the facts described in the notification;
- Data processors that may be appointed from time to time;
- Data Protection Officer

Whistleblowers, affected persons and the other parties involved may obtain further information on the processing of the personal data provided at privacy@esprinet.com (for Esprinet Ibérica, S.L.U. and Esprinet Portugal, LdA) or at privacy@v-valley.com (for V-Valley Advanced Solutions España). You may also contact

the Data Protection Officer of the Esprinet Group in Spain at the following e-mail address: dpo@esprinet.com.

9. OTHER DETECTION SYSTEMS

9.1. 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, a preliminary assessment shall be carried out in accordance with this policy.

9.2. 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.

In such a case, when the customer's complaint consists of the potential committing of a breach of regulations internal and/or external to the Esprinet Group, this must be notified through the information channels provided by the Company and cited in section 8.1 of this Policy.

In addition, as previously reported, infringements may also be reported through the information channels adopted by the competent public authorities, whether at national or at regional level.

10. PROTECTION OF THE WHISTLEBLOWER

The Esprinet Group recognises certain rights of persons who adopt the position of whistleblower, as soon as the Company receives the information notified by the whistleblower. In this way, the confidentiality of any data provided and the confidentiality of the whistleblower's identity and/or the anonymity of the whistleblower will be guaranteed when the whistleblower has so decided. These rights shall be guaranteed during the entire processing of the file in question.

Except in cases of criminal liability for libel or defamation (in such cases, the Company shall inform the whistleblower prior to any disclosure of his or her identity, unless such disclosure would prejudice the ongoing investigation or legal proceedings), the identity of the whistleblower shall be protected at every stage of the breach management process. Therefore, the identity of the whistleblower cannot be disclosed without his or her express consent and all those receiving or involved in the handling of notifications are obliged to protect his or her confidentiality.

The breaching of the obligation of confidentiality shall represent a serious disciplinary infringement.

In the same way, any form of retaliation or discrimination against the whistleblower and the affected persons shall constitute a serious disciplinary offence.

In any case, retaliatory or discriminatory dismissal of the person reporting the facts that are the subject of the

offence shall be null and void. The modification of labour rights shall also be null and void.

Lastly, in case of disputes relating to the imposing of disciplinary sanctions or the demotion, dismissal, transfer or submission of the whistleblower to another organisational measure with direct or indirect negative effects on working conditions, it is the responsibility of the company to prove that such measures are in no way a consequence of the notification itself.

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;

11. PROTECTION OF THE AFFECTED PERSON

In the same way that the Esprinet Group guarantees respect for the rights of whistleblowers, it also recognises a number of rights in favour of the affected persons, i.e. those persons who are alleged to have committed an internal and/or external breach of regulations.

In this regard, the Company conducts this Policy taking into account the right to judicial protection and defence, access to the file under the terms of the applicable laws, confidentiality and, in particular, the presumption of innocence.

The affected person has the right not to have his or her identity disclosed without his or her express consent, except where this is a necessary and proportionate obligation imposed by law or in the course of an investigation within the framework of judicial proceedings. The affected person has the right to a trial without undue delay and with all the guarantees.

The affected person has the right to know that there is a report of an offence against him for her and shall be informed of the same as soon as possible, provided that it does not jeopardise the investigation, and prior to his or her statement.

12. INFORMATIONS FLOWS TO THE MONITORING BODY

Any person who becomes aware of infringements of this Policy by Recipients should immediately notify the Supervisory Body of the specific Company or, in accordance with Policy DIS01001 Policy for the Prevention of Fraud and Infringement of the Code of Ethics and for the Handling of Whistleblowing Complaints, submit a report through the whistleblowing platform.

13. COMPLIANCE

Failure to comply with ethical rules and standards will compromise the Esprinet Group. For this reason, all Employees must be familiar with and observe the contents of this Policy.

Failure to comply with the contents of this Policy and the Organisation and Management Model, the Code of Ethics and the company's internal regulations may lead to the imposing of sanctions, proportional to the seriousness of the actions, as provided in the applicable labour regulations or the consequences indicated in the contractual clauses.

14. 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.