MINDSOFT

ANTI-BRIBERY POLICY OF MINDSOFT IT SOLUTIONS SRL

I. INTRODUCTION

1.1 BACKGROUND

Whereas, in the course of its activity, the company takes part in public procurement procedures organised by public authorities, comes into contact with public officials and thus operates in an area with an increased risk of corruption.
Whereas the company has contractual relationships with business partners that have implemented anti-corruption policies and programmes.
Whereas it is necessary to minimise the risks that may affect the company's image.
It has been decided to adopt this anti-corruption policy, which aims to prevent corruption within the company and in its relations with public authorities and other business partners, and which is mandatory for the company's managers, employees, representatives and contractors and for any other persons acting on behalf of the company.
This anti-corruption policy will also be brought to the attention of business partners by publication on the company's website, www.mindsoft.ro

1.2 PURPOSE

The aim of Mindsoft IT Solutions is to provide high-quality services while upholding the principles of ethics and integrity, to meet the requirements of interested parties and to continually improve the effectiveness of the Anti-Bribery Management System. To this end, a series of analytical and constructive measures have been taken which, together, will lead to the achievement of this objective.
The constructive measures include: a process-based approach that makes it possible to identify and resolve integrity deviations in the activities carried out; methods for identifying and preventing bribery situations; internal reviews and reviews with external interested parties; the use of appropriate policies and procedures, etc.
The analytical measures include control methods, at all their stages, aimed at identifying and eliminating deviations related to bribery or to the anti-bribery management system.

II. SCOPE

1. The procedure applies to persons who make reports and who have obtained information on breaches of the law in a work-related context, in the course of the activity carried out within the Company.
2. These persons include, at a minimum, the following:

- **workers**
- **self-employed persons within the meaning of Article 49 of the Treaty on the Functioning of the European Union**
- **shareholders and persons belonging to the administrative, management or supervisory body of the Company,**
- **volunteers and paid or unpaid trainees**
- **any person working under the supervision and direction of the Company, its subcontractors and its suppliers**

- **persons whose employment relationship has not yet begun and who report through internal or external reporting channels or publicly disclose information on breaches of the law obtained during the recruitment process or other pre-contractual negotiations, or where the employment or service relationship has ended.**
- **persons who report or publicly disclose information on breaches of the law anonymously**.

3. The strategic objective of our anti-bribery policy is that, year after year, performance in ethics and integrity remains at an appropriately high level. To this end, the anti-bribery management system provides methods for monitoring actual or potential issues in order to track how they develop. Specific objectives are also set out in Management Programmes, which are reviewed periodically to ensure that they are achieved. As an organisation that wishes to operate to the high standards of ethics and integrity required by the public and other interested parties, we maintain a policy of continual improvement of our actions and measures to combat bribery. The staff responsible for ethics and integrity periodically review the management system to ensure its continuing suitability, adequacy and effectiveness. Ethics and integrity must be the concern of every person in the organisation. Mindsoft IT Solutions believes that excellence is achieved by building awareness of ethics and integrity among all employees and, to this end, will educate and train its staff in all aspects required to keep the anti-bribery management system under control. The Anti-Bribery Officer (the anti-bribery compliance function) has the responsibility and authority to verify, implement and maintain the anti-bribery policy at all levels of the organisation.

III. DEFINITIONS

For the purposes of this procedure, the terms below have the following meanings:

1. **breaches of the law** - acts or omissions that constitute non-compliance with legal provisions in areas such as: public procurement; financial services, products and markets, and prevention of money laundering and terrorist financing; product safety and compliance; transport safety; protection of the environment; radiation protection and nuclear safety; food and feed safety, animal health and welfare; public health; consumer protection; protection of privacy and personal data, and security of network and information systems; breaches affecting the financial interests of the European Union; breaches relating to the internal market, including breaches of European Union competition and State aid rules, as well as breaches relating to the internal market in relation to acts which breach the rules of corporate tax or arrangements whose purpose is to obtain a tax advantage that defeats the object or purpose of the applicable corporate tax law, which constitute disciplinary offences, administrative offences or criminal offences, or which defeat the object or purpose of the law;
2. **information on breaches of the law** – information, including reasonable suspicions, about actual or potential breaches of the law which have occurred or are very likely to occur within the Company, where the public interest whistleblower works or has worked or with which they are or have been in contact through their work, as well as information about attempts to conceal such breaches;
3. **reporting** - the oral or written communication of information, in accordance with the methods set out in Article 5(4) of Law 361/2022, on any act that constitutes a breach of the law;
4. **internal reporting** - the oral or written communication of information on breaches of the law within the Company. Internal reporting is made through the means provided by the Company for reporting breaches of the law, which constitute the internal reporting channels;
5. **public disclosure** - making information on breaches of the law available in the public domain, by any means;
6. **public interest whistleblower** - a natural person who reports or publicly discloses information on breaches of the law obtained in a work-related context;
7. **facilitator** - a natural person who assists a public interest whistleblower in the reporting process in a

work-related context, and whose assistance must be confidential;
8. **work-related context** - current or past work activities of any kind, paid or unpaid, carried out within the Company, through which persons may obtain information on breaches of the law and may suffer retaliation if they report them;
9. **worker** - a natural person in an employment or service relationship, under general or specific legal provisions, who performs work in return for remuneration;
10. **person concerned** - a natural or legal person referred to in the report or public disclosure as the person to whom the breach of the law is attributed or with whom that person is associated;
11. **retaliation** - any direct or indirect act or omission occurring in a work-related context which is prompted by internal or external reporting or by public disclosure and which causes or may cause harm to the public interest whistleblower;
12. **follow-up actions** - any action taken by the designated person to resolve the report and, where applicable, to remedy the reported breach;
13. **feedback** - providing the public interest whistleblower with information on the follow-up actions and the reasons for them;
14. **designated person (the Company's Whistleblowing Policy Officer)** - the officer with the duties set out in this procedure, appointed within the Company by Decision of the Administrator
15. **bribery** - giving or offering an advantage or anything of value, directly or indirectly, to a person in order to induce that person or another person to carry out an activity or perform a function improperly. Bribery also means requesting or receiving an advantage or anything of value, directly or indirectly, from a person with the intention that a relevant activity or function will be carried out improperly, by you or by another person. You must never take part in taking or giving a bribe. A bribe may be financial or of another nature and may include offering or receiving money, loans, contributions or donations, travel, job offers, refunds, discounts, goods, services or anything else that may be considered of value. Gifts or entertainment may be interpreted as forms of bribery in certain circumstances. A bribe may also take the form of a “reward” paid after the improper performance of a particular obligation or duty.

IV. WORKING PROCEDURE

1. General

Mindsoft IT Solutions maintains an anti-bribery management system in accordance with the requirements of the ISO 37001:2016 standard. The anti-bribery policy is maintained as documented information within the organisation. The policy has been communicated to all Mindsoft IT Solutions employees during training on the implementation of the anti-bribery management system and is available to relevant interested parties through publication on the internal server and by direct notification, as appropriate.
The Executive Director ensures that the anti-bribery policy:
- is appropriate to the purpose of the organisation;
- supports the commitment to meet the requirements of interested parties and to continually improve the effectiveness of the ABMS;
- provides a framework for setting and reviewing objectives; -
is communicated and understood within the organisation through display and training;
- is updated periodically. In order to achieve its objectives of preventing and combating bribery.

2. Objectives

The anti-bribery objectives are set by the Executive Director and are documented in management programmes. They are expressed in measurable terms and focus on the following strategic aspects

established through management commitment:
- Complaints/reports from interested parties concerning bribery, corruption and other integrity issues Actual or suspected incidents of corruption
Value of financial losses or criminal acts caused by bribery incidents
- Criminal convictions for bribery, corruption or similar cases.
Taking these aspects into account, measurable objectives are set and documented for all relevant functions within the Anti-Bribery Management Programme, which contains actions, resources, deadlines and responsibilities for achieving the objectives. Any changes to the ABMS will be made in a planned manner, taking into account the following:
- The need for changes and their potential consequences;
- The integrity of the ABMS;
- The availability of resources.

3. The general principles governing the protection of reports on breaches of the law are the following:
a) **the principle of legality**, according to which authorities, public institutions, other legal persons governed by public law and legal persons governed by private law are obliged to respect fundamental rights and freedoms by ensuring full respect for, among others, freedom of expression and information, the right to protection of personal data, the freedom to conduct a business, the right to a high level of consumer protection, the right to a high level of human health protection, the right to a high level of environmental protection, the right to an effective remedy and the right of defence;
b) **the principle of accountability**, according to which the public interest whistleblower is obliged to provide data or information on the reported facts;
c) **the principle of impartiality**, according to which reports are examined and resolved without bias, regardless of the beliefs and interests of the persons responsible for resolving them;
d) **the principle of good administration**, according to which public authorities and institutions and other legal persons governed by public law must carry out their activity in the general interest, with a high degree of professionalism and with efficient and effective use of resources;
e) **the principle of balance**, according to which no person may rely on the provisions of this procedure to reduce an administrative or disciplinary sanction for a more serious act of their own that is unrelated to the report;
f) **the principle of good faith**, according to which protection is given to a person who had reasonable grounds to believe that the information on the reported breaches was true at the time of reporting and that such information fell within the scope of Law No. 361/2022 and of this procedure;

4. Acts constituting breaches of the law
(1) Acts or omissions that constitute non-compliance with legal provisions concerning all areas of activity within the Company, as well as areas such as:
- public procurement;
- financial services, products and markets, and prevention of money laundering and terrorist financing;
- product safety and compliance;
- transport safety;
- protection of the environment;
- radiation protection and nuclear safety;
- food and feed safety, animal health and welfare;
- public health;
- consumer protection;

- protection of privacy and personal data, and security of network and information systems, as set out in Annex No. 2; breaches affecting the financial interests of the European Union, as referred to in Article 325 of the Treaty on the Functioning of the European Union and as further specified in relevant European Union measures; breaches relating to the internal market, as referred to in Article 26(2) of the Treaty on the Functioning of the European Union, including breaches of European Union competition and State aid rules, as well as breaches relating to the internal market in relation to acts which breach the rules of corporate tax or arrangements whose purpose is to obtain a tax advantage that defeats the object or purpose of the applicable corporate tax law, which constitute disciplinary offences, administrative offences or criminal offences, or which defeat the object or purpose of the law;

(2) The list of areas in which breaches may occur is not exhaustive. Therefore, any act that constitutes a breach of the law, or even a reasonable suspicion of actual or potential breaches of the law, including information on breaches that have occurred or are very likely to occur within the Company, may be reported.
(3) The persons referred to in point 2 must not make payments or grant any other advantages to Public Officials beyond those provided for by law or local regulations in order to obtain an approval, licence or other necessary authorisation. This situation may sometimes arise when the Organisation wishes to build, convert or extend a site and needs to obtain certain approvals for its activity (for example, for a change of use of an existing building). Particular attention will be paid to: situations in which an inspector offers to carry out an undocumented on-the-spot inspection for a certain sum of money.
Planning ahead: To avoid this type of situation, the following provisions must be observed:
• The person must be informed of the requirements for obtaining the approval and of the Organisation's progress in meeting them;
• Problems will be resolved proactively, so that there is enough time to obtain the approvals without being under the pressure of an investigation;
• Maintaining good relations with the authorities;
• Explaining very clearly that the Organisation never offers bribes as a business practice;
• Working with other people in the industry who face similar problems and who follow similar ethical standards;
• Justifying the reasons why the Organisation is entitled to obtain the requested approval or licence, mentioning, among other things, the benefits that the Organisation's presence in the region brings to local communities.
• No money will be paid and no other advantage will be offered to Government Officials to avoid an inspection, to influence the results of an inspection or to avoid a fine. During an inspection, a polite but correct attitude will be maintained towards the Government Official carrying it out, without offering them anything of value or any advantage before, during or after the inspection.

(4) Public Officials are employees or representatives of a government or of an entity owned or controlled by a government anywhere in the world, including senior or other government employees. Government-owned or government-controlled entities include, but are not limited to, central banks, state-guaranteed funds, state hospitals and any other companies owned or controlled by a government entity;
• Any person who holds a legislative, administrative or judicial position, whether appointed or elected to that position;
• Any candidate for public office;
• Any official of a political party;
• Any official, employee, representative or agent of a public international organisation, such as the United Nations or the World Bank;
• Any member of a royal family;
• Any child, spouse, parent, sibling or other relative of the persons mentioned above.

It is the responsibility of every person covered by this Policy to know whether a person with whom they have business dealings is a Government Official. In case of doubt, the HR Department or the management team may be consulted.

(5) The prior written approval of Management must be obtained before any political contribution can be authorised or made on behalf of the Organisation.

(6) The Organisation is liable for bribes paid by third parties acting on its behalf or by its employees or other persons providing services to the Organisation. Therefore, no person will authorise or ask employees or third parties to pay a bribe to any person (including Public Officials) or to accept a bribe from anyone. Likewise, activities carried out by third parties acting on behalf of the Organisation that you suspect may conflict with this Policy must not be overlooked. Persons covered by this policy have a duty to bring such matters to the attention of the management team immediately. Particular care will be taken when assessing a potential employee or third party who may act on behalf of the Organisation, especially if that person will interact with Public Officials on behalf of the Organisation.

(7) All payments and expenses must be recorded fully and appropriately in accordance with the applicable accounting rules. These include, but are not limited to, the following:
• Gifts
• Travel and entertainment expenses
• Sponsorship expenses
• Political contributions
• Payments to third parties, suppliers and service providers
Records must be kept in accordance with all prior measures and relevant approvals required under this Policy.

(8) All persons covered by this policy are obliged to comply with the ethical standards set by the Policy and must take responsible measures to prevent breaches of it. In the event of a wilful breach of the anti-bribery provisions, the legal provisions on disciplinary investigation will apply. Breaches of the anti-bribery provisions may also be reported to the police and may result in criminal proceedings against the person found guilty. Taking or giving a bribe is a criminal offence punishable by imprisonment.

5. Reporting methods

(1) Reporting acts considered to be breaches of the law must be seen as the exercise of a professional duty. If an employee suspects breaches of the law that have occurred, are occurring or are about to occur and that may affect the interests of the Company, the employee must act immediately under this procedure and is protected against any discrimination.
(2) Persons who report breaches of the law that have occurred or are very likely to occur within the Company have the following reporting methods available:

- **internal channels** – within the Company
- **public disclosure** – the press, professional organisations, trade unions or employers' organisations, non-governmental organisations, parliamentary committees, etc. (for more details, see Chapter V of Law No. 361/2022);

(3) Within the Company, acts constituting breaches of the law are reported mainly through the existing internal reporting channels.
(4) To protect the confidentiality of the identity of the public interest whistleblower and of any third party mentioned in the report, and to prevent access to the report by unauthorised staff, within the Company

reports of acts constituting breaches of the law are sent to a single employee designated by Decision of the Company's administrator, namely *the Company's Whistleblowing Policy Officer (the "designated person").*
(5) The Company's Whistleblowing Policy Officer is responsible for receiving, recording and examining reports, diligently carrying out follow-up actions and resolving reports. The Company's Whistleblowing Policy Officer must act impartially and be independent in carrying out these duties.
(6) Reports are made in writing, on paper or electronically, by telephone or through other voice messaging systems, or in a face-to-face meeting at the request of the public interest whistleblower.
(7) Written reports, on paper or electronically, are made by completing the reporting form (***Annex 1***) and must contain at least the following information:

- the first name, last name and contact details of the public interest whistleblower, including email address;
- the work-related context in which the information was obtained;
- the person concerned, if known;
- a description of the act likely to constitute a breach of the law within the Company;
- the data or evidence supporting the alleged breach of the law within the Company;
- the date;
- the signature.

(8) By way of exception from paragraph (7), a report that does not contain the first name, last name, contact details or signature of the public interest whistleblower is examined and resolved to the extent that it contains indications of breaches of the law.
(9) The reporting form (***Annex 1***) completed on paper will be placed in an envelope marked "*Report of breach of the law*" and submitted to the box specially set up for correspondence on public interest whistleblowing reports, located on the Company's intranet. The electronically completed form will be sent to the email address of the Whistleblowing Policy Officer.
(10) Only the Company's Whistleblowing Policy Officer has access to the box set up for submitting public interest whistleblowing reports and to the email address, and must check the box and the email regularly. Emails are printed and follow the procedure applicable to reports made on paper.

(11) Information about the Company's Whistleblowing Policy Officer and the internal reporting methods will be published on the Company's website and displayed at its registered office, in a visible and accessible place. At least one reporting method must be accessible at all times.
(12) Reports are recorded in a register, using the form in ***Annex 2****;* the register contains **the date the report was received, the first name, last name and contact details of the public interest whistleblower, the subject of the report and how it was resolved**, is kept in electronic format and will be password-protected.
(13) Where a telephone line or another voice messaging system on which conversations cannot be recorded is used for reporting, the Whistleblowing Policy Officer must prepare minutes containing a complete and accurate transcript of the conversation. The Whistleblowing Policy Officer gives the public interest whistleblower the opportunity to check, correct and agree to the minutes of the conversation by signing them.
(14) Where the public interest whistleblower requests that the report be made in the presence of the Whistleblowing Policy Officer, the officer must prepare minutes in a durable and accessible form, subject to the consent of the public interest whistleblower. The Whistleblowing Policy Officer gives the public interest whistleblower the opportunity to check, correct and agree to the minutes of the conversation by signing them.
(15) Within no more than 7 calendar days of receiving the report, the Whistleblowing Policy Officer must send the public interest whistleblower an acknowledgement of receipt of the report (in electronic format).

(16) The Whistleblowing Policy Officer must inform the public interest whistleblower and the Company's Administrator of how the report was resolved.
(17) Reports are kept for 5 years. After the 5-year retention period expires, they are destroyed, regardless of the medium on which they are kept, and destruction minutes are drawn up.

6. Closure of internal reports

(1) A report is closed when it does not contain its essential elements, other than the identification data of the public interest whistleblower, and the Whistleblowing Policy Officer has requested that it be completed within 15 days, without this obligation being fulfilled.
(2) A report is closed when it is submitted anonymously or does not contain enough information on breaches of the law to allow it to be analysed and resolved, and the Whistleblowing Policy Officer has requested that it be completed within 15 days, without this obligation being fulfilled.
(3) The closure decision is communicated to the public interest whistleblower, stating the legal grounds.

(4) The Whistleblowing Policy Officer may decide to close the procedure if, after examining the report, it is found that the breach is clearly minor and requires no further follow-up actions other than closing the procedure. This provision does not affect the obligation to maintain confidentiality or to inform the public interest whistleblower, nor does it affect other obligations or other applicable procedures for remedying the reported breach.

7. Confidentiality of the identity of the public interest whistleblower

(1) The Whistleblowing Policy Officer must not disclose the identity of the public interest whistleblower or any information that would allow them to be identified directly or indirectly, unless the whistleblower has given express consent.

(2) By way of exception from paragraph (1), the identity of the public interest whistleblower and any other information referred to in paragraph (1) may be disclosed only where this is an obligation imposed by law, subject to the conditions and limits it sets.

(3) In the case referred to in paragraph (2), the public interest whistleblower is informed in advance, in writing, of the disclosure of their identity and of the reasons for disclosing the confidential data concerned. This obligation does not apply where informing the whistleblower would jeopardise investigations or judicial proceedings.

(4) The obligation to maintain confidentiality also applies where a report reaches, by mistake, an employee of the Company other than the Whistleblowing Policy Officer. In this case, the report is forwarded immediately to the Whistleblowing Policy Officer.

(5) Personal data that is not necessary for resolving a specific report is not collected or, if collected accidentally, is deleted.

8. Measures to protect the public interest whistleblower

(1) The Company ensures that a whistleblower who reports any breach of the law is adequately protected,

as provided by law, against possible negative consequences, such as retaliation, discrimination or any form of unfair treatment.
(2) A public interest whistleblower who reports or publicly discloses information on breaches of the law does not breach legal provisions or contractual clauses on the disclosure of information and is not liable for reporting or publicly disclosing such information, provided that they made the report or public disclosure in accordance with the law and had reasonable grounds to believe that the report or disclosure was necessary to reveal a breach of the law.
(3) A public interest whistleblower who acquires or accesses data and information they know of by virtue of their job duties or employment relationship is not liable if the purpose of the acquisition or access is to report or publicly disclose a breach of the law, and the report or public disclosure was made in accordance with the law.
(4) The liability of public interest whistleblowers for acts or omissions that are unrelated to the report or public disclosure, or that are not necessary to reveal a breach of the law, is subject to general law.
(5) **Any form of retaliation against public interest whistleblowers is prohibited**, **as are threats of retaliation or attempted retaliation, in particular those concerning:**
a) any suspension of the individual employment contract;b) dismissal;c) amendment of the employment contract;

d) reduction in salary and change of working hours;
e) demotion or obstruction of promotion and professional development, including through negative assessments of individual work performance or negative references for the work carried out;
f) any other disciplinary sanction;
g) coercion, intimidation, harassment;h) discrimination, other disadvantage or unfair treatment;

i) refusal to convert a fixed-term employment contract into a permanent employment contract, where the worker had legitimate expectations of being offered permanent employment;j) refusal to renew a fixed-term employment contract or early termination of such a contract;k) harm, including to the person's reputation, particularly on social media, or financial loss, including loss of business opportunities and loss of income;

l) blacklisting on the basis of a sector-wide or industry-wide agreement, formal or informal, which may mean that the person will not find employment in that sector or industry in the future;m) unilateral out-of-court termination of a contract for goods or services, without the conditions for doing so being met;n) cancellation of a licence or permit;

o) a request to undergo a psychiatric or medical assessment.
(6) The public interest whistleblower may challenge the measures referred to in paragraph (5) by an application to the competent court, depending on the nature of the dispute, in whose territorial jurisdiction the whistleblower is domiciled.
(7) At the request of a public interest whistleblower who is subject to a disciplinary investigation following internal reporting or public disclosure, the disciplinary committees must invite the press and a representative of the trade union or professional association, or a representative of the employees, as appropriate. The announcement is made by a notice on the organisation's own website at least 3 working days before the meeting, failing which the report and the disciplinary sanction applied are null and void.

9. Protection of the identity of the person concerned and of third parties

(1) The rules on identity protection applicable to public interest whistleblowers also apply to the person concerned and to third parties referred to in the report.

(2) The identity of the person concerned is protected while the follow-up actions to the report or public disclosure are ongoing, except where, as a result of resolving the report or disclosure, it is found that the person concerned is not guilty of the breaches of the law that were the subject of the report or disclosure.

(3) Persons concerned have the right of defence, including the right to be heard and the right of access to their own file.

VI. RESPONSIBILITIES

1. Whistleblowing Policy Officer

(1) The Whistleblowing Policy Officer is the person designated within the Company to receive, record and examine reports, carry out follow-up actions and resolve reports, and must act impartially and be independent in carrying out these duties.

(2) Ensures that information on their contact details, as well as the internal and external reporting methods, is published on the Company's website and displayed at its registered office, in a visible and accessible place, and that at least one reporting method is accessible at all times.

(3) Receives reports submitted through the internal channels and complies with the deadlines set in this procedure, being aware that obstructing reporting by any means is an administrative offence and is sanctioned under Law No. 361/2022 on the protection of public interest whistleblowers.

(4) Records reports in the electronic Register.

(5) Diligently carries out follow-up actions.

(6) Must inform the public interest whistleblower and the Company's Administrator of how the report was resolved, or whether the breaches of the law concern the administrator himself.

(7) After the 5-year retention period expires, ensures that reports are destroyed on the basis of destruction minutes, regardless of the medium on which they are kept.

(8) Has a professional obligation to keep confidential the data of the whistleblower, the person concerned and any third parties referred to in the report, being aware that disclosing this information is an administrative offence and is sanctioned under Law No. 361/2022 on the protection of public interest whistleblowers.

2. Public interest whistleblower

(1) Acts in good faith, being convinced of the reality of the facts or that the act constitutes a breach of the law, knowing that reporting untrue facts is an administrative offence and is sanctioned under Law No. 361/2022 on the protection of public interest whistleblowers.

VII. FORMS

ANNEX 1 - Reporting of acts constituting breaches of the law

ANNEX 2 - Register

MINDSOFT

ANNEX 1

REPORTING OF ACTS CONSTITUTING BREACHES OF THE LAW

- *We assure you that we take all information received seriously and we guarantee the confidentiality of the information provided in your report, as the designated person is bound by a duty of confidentiality, in accordance with applicable law.*
- *The designated person must NOT disclose the identity of the whistleblower or any information that would allow you to be identified, except where this is an obligation imposed by law, in which case you will be notified in writing, before disclosure, of the disclosure of your identity and of the reasons for disclosing the confidential data concerned.*
- *You will not be informed of the disclosure where informing you would jeopardise investigations or judicial proceedings.*
- *Furthermore, the obligation to maintain confidentiality does not apply where the whistleblower has intentionally revealed their identity in the context of a public disclosure.*
- *The Company ensures that a whistleblower who reports any breach of the law is adequately protected, as provided by law, against possible negative consequences, such as retaliation, discrimination or any form of unfair treatment.*

FIRST NAME, LAST NAME AND CONTACT DETAILS OF THE PUBLIC INTEREST WHISTLEBLOWER
WORK-RELATED CONTEXT IN WHICH THE INFORMATION WAS OBTAINED
PERSON CONCERNED, IF KNOWN **Full name/Position/Organisational unit**
DESCRIPTION OF THE ACT LIKELY TO CONSTITUTE A BREACH OF THE LAW WITHIN THE COMPANY
DATA OR EVIDENCE SUPPORTING THE ALLEGED BREACH OF THE LAW WITHIN THE COMPANY

MINDSOFT

Date of report	Signature

MINDSOFT

ANNEX 2

REGISTER **Confidential**					
Report No.	**Date of receipt of the report**	**Whistleblower who reported the act (Last name/First name)**	**Contact details of the public interest whistleblower**	**Subject of the report**	**Resolution**