WHISTLEBLOWER POLICY REGARDING

NETCOMPANY - INTRASOFT SA GREEK BRANCH WHISTLEBLOWER ARRANGEMENT

Dated: 18/11/2022

WHISTLEBLOWER POLICY

1 INTRODUCTION AND PURPOSE

1.1 This Whistleblower Policy describes the purpose of Netcompany – Intrasoft SA Greek Branch (hereinafter referred to as "Intrasoft") having introduced a Whistleblower Arrangement , how it works, who can make use of the aforementioned Arrangement, and what may be reported through such Arrangement.

1.2 The purpose of the Whistleblower Arrangement is to ensure that a Whistleblower, as defined in this Whistleblower Policy, can swiftly and confidentially, through a special, independent and autonomous channel, report violations or potential violations, allowing an independent and autonomous whistleblower unit to assess which steps are required in this respect.

1.3 Intrasoft has established a whistleblower arrangement within the scope of the EU Directive 2019/1937 and the Greek Law No. 4990/2022 on the protection of persons reporting violations of EU law (hereinafter referred to as the " **Arrangement**").

2 WHO CAN USE THE ARRANGEMENT?

2.1 The Arrangement can be used by persons who report information on violations to which the person in question has gained access in connection with his or her work-related activities, and who belong to the following categories of persons (hereinafter referred to as "**Whistleblower**"):

(i) Employees

(ii) Self-employed persons, non-salaried employees, consultants

(iii) Shareholders, General Managers, members of the board of directors, or similar governing body in an undertaking.

(iv) Volunteers

(v) Paid or unpaid trainees

(vi) Persons working under the supervision and management of contracting parties, subcontractors, and suppliers.

(vii) Persons who are reporting or publishing information to which they have gained access in a work-related relationship that has ceased since then.

(viii) Persons in work-related relationships that have not yet commenced, who report information on violations to which they have gained access during the course of the recruitment process or other pre-contractual negotiations.

2.2 Persons listed under section 9.4 can also file reports under the Arrangement (for instance an intermediary assisting the Whistleblower with the reporting process in a work-related context).

2.3 Persons not included in the categories of persons stated in sections 2.1 or 9.4 cannot file reports under the Arrangement but they have to report through ordinary communication channels.

3 WHAT MAY BE REPORTED THROUGH THE ARRANGEMENT?

3.1 The Arrangement is open for reports regarding violations of EU law within the scope of application of the Whistleblower Directive and the National Law (see section 3.4 (i)) as well as reports regarding serious offences or other serious matters (see section 3.4 (ii)).

3.2 "Violations" means acts or omissions that

a) are illegal or constitute a serious offence or other serious matters comprised by section 3.4; or

b) allow circumventions of the purpose of the rules under section 3.4.

3.3 Any information may be reported, including reasonable suspicion about actual or potential violations or serious matters comprised by section 3.4 which have occurred or most probably will occur at Intrasoft, as well as any attempts to cover up such violations.

3.4 The report must concern violations or potential violations defined as acts or omissions which are unlawful under EU law or contrary to the subject or purpose of the rules of EU law falling within the scope of L. 4990/2022. In particular, the report must relate to infringements which:

(i) are serious offences or other serious matters, like for instance:

- Violation of any duty of confidentiality
- Abuse of financial means
- Theft
- Deceit
- Embezzlement
- Fraud
- Bribery
- Violation of industrial safety rules
- Any form of sexual harassment
- Severe harassment, e.g. bullying, violence, and harassment due to race, political or religious affiliation.

(ii) are illegal pursuant to EU law within the following areas: :

- public procurement

- financial services, products, and markets, as well as the prevention of money laundering and the financing of terrorism,

- product safety and compliance,

- transport safety,

- environmental protection,

- radiation protection and nuclear safety,

- food and feed safety, as well as animal health and welfare,

- public health,

- consumer protection,

- protection of privacy and personal data, as well as the security of network and information systems.

3.5 The Arrangement may only be used for reporting violations or potential violations in relation to the issues described in section 3.4 that have occurred or most probably will occur in Intrasoft's organisation, committed for instance by employees, executive board, or members of the board of directors of Intrasoft**.** In connection with reports on incidents committed by Intrasoft, please note

that such incidents may be reported although the incident cannot be attributed to an individual person but may be due to a basic systemic failure at Intrasoft.

3.6 Offences that are not comprised by the Arrangement must be reported through ordinary communication channels.

4 CONTENTS OF THE REPORT

4.1 To facilitate further investigation of the reported issue, and to be able to identify the offence, it is important that the Whistleblower describes the offence in the best possible way. It is thus not possible to make any further investigations of a report if the report is not specified or if it only contains very general allegations without any further clarification.

4.2 Therefore, it is important that the Whistleblower - to the utmost extent - provides the following information:

- a description of the matter;
- the person(s) involved;
- whether others are aware of the suspicion about the matter;
- whether the executive board knows about the matter;
- whether documents exist that support the matter;
- whether and where further information may be found about the matter;
- for how long the matter has gone on; and
- whether the Whistleblower knows about any attempts to hide the offence.

4.3 Manifestly unfounded reports will not be investigated further.

5 HOW CAN A REPORT BE SUBMITTED AND WHO IS TO RECEIVE THE REPORT?

5.1 Intrasoft has appointed a unit responsible for the receipt and monitoring of the reports (hereinafter referred to as the "whistleblower unit") that

(a) will receive the reports and be in contact with the Whistleblower;
(b) will follow-up on the reports; and
(c) give feedback to the Whistleblower.

5.2 The whistleblower unit in charge of the tasks mentioned in section 5.1 consists partly of two lawyers from Plesner Law Firm (hereinafter "**Plesner**"), and partly of an impartial group of persons at Intrasoft.

5.3 Written reports are submitted through the Whistleblower Arrangement that can be found on Intrasoft's website:

https://www.netcompany-intrasoft.com/whistleblower

5.4 Written reports are received by two lawyers at Plesner Law Firm. Plesner will make a legal capacity assessment of the persons of the whistleblower unit who are able to process the report, after which the report will be forwarded to the relevant persons (hereinafter referred to as **"Report Monitoring Officers"**) at Intrasoft. Before forwarding the report, Plesner will assess whether the report falls within the scope of application of the Arrangement.

5.5 It is only possible to submit written reports under the Arrangement.

5.6 The whistleblower unit will treat all written reports as confidential.

5.7 The Report Monitoring Officers appointed to receive and follow up on the reports are subject to a duty of confidentiality regarding the information contained in the reports.

5.8 As an exemption to the above, the reports that concern violations or potential violations defined as acts or omissions which are serious offences or other serious matters, like for any form of sexual harassment, severe harassment, e.g. bullying, violence, and harassment due to race, political or religious affiliation, are covered by the "Policy on Preventing and Combating Violence and Harassment in the Workplace" which has been adopted by the Company in accordance with article 9 of the Greek Employment Law 4808/2021. This policy stipulate the people who will be responsible, with the assistance of other members of the relevant Department of the Company, to receive the reports, as well as to provide guidance and information to the employees in order to prevent and deal with incidents of violence and harassment in the workplace.

6 ANONYMITY

6.1 Intrasoft encourages the Whistleblowers to state their name when submitting a report so that the Report Monitoring Officers are able to ask clarifying questions and subsequently provide feedback on the further course of the investigation. However, anonymous communication between Plesner and a Whistleblower who chooses to be anonymous is possible (see section 6.4 and 6.5).

6.2 If the Whistleblower chooses to submit an anonymous report, it is recommended - to ensure full anonymity - that the Whistleblower uses a private PC or, for instance, a PC located at a public library.

6.3 Plesner will make a communication module available, allowing the Whistleblower to communicate with Plesner for the purpose of providing additional information about the reported issue, which Plesner will then pass on to the Report Monitoring Officers.

6.4 If the Whistleblower chooses to submit an anonymous report, it is possible for the Whistleblower to communicate with Plesner through the communication module. The Whistleblower can provide additional information to Plesner through the communication module and remain anonymous. In connection with the reporting, a one-off code is generated which, in order to safeguard the anonymity, cannot be re-created. Therefore, it is **important** that the Whistleblower keeps the code and remembers to log on the communication module to communicate with the whistleblower unit.

6.5 The communication module can be accessed through the above-mentioned link under the Arrangement (see section 5.3) to log on the communication module. If the Whistleblower chooses to be anonymous, it is important that the Whistleblower regularly enters the communication module to check whether Plesner has asked any questions. If the Whistleblower is anonymous, Plesner is not able to encounter the Whistleblower in any other ways, for instance to inform the Whistleblower that additional questions etc. have been submitted.

7 INFORMATION TO THE WHISTLEBLOWER

7.1 The Whistleblower will receive:

- an acknowledgement of receipt of the report within seven (7) working days of that receipt; and
- feedback soonest possible and in principle within three (3) months from the acknowledgement of receipt of the report or if no confirmation has been sent to the Whistleblower, within three (3) months after the expiry of seven (7) working days from the submission of the report.

7.2 "Feedback" means a notification about the measures taken by Intrasoft to assess the correctness of the allegations made in the report and, where relevant, to counter the reported offence. The

feedback provided by the whistleblower unit must, at any time, observe the rules under data protection law, which may entail limitations in relation to the contents of the feedback to the Whistleblower.

7.3 Depending on the circumstances, an extension of the timeframe for the feedback may be required, where necessary due to the specific circumstances of the case, in particular the nature and complexity of the report, which may require a lengthy investigation. If this is the case, the Whistleblower must be notified in this respect.

8 INFORMATION TO AND PROTECTION OF THE PERSON CONCERNED

8.1 After a preliminary investigation has taken place and all relevant evidence has been secured, the reported person will for instance be informed about:

- the identity of the Report Monitoring Officer(s) responsible for the investigation of the report; and
- the issues of the report.

8.2 The reported person is entitled to protection of his or her identity during the case management and has a right to effective defence. These rights may not be waived by agreement to the detriment of the reported person.

8.3 Under certain circumstances, the reported person will also have the right of access to information about the Whistleblower's identity where necessary for the reported person to exercise his or her right to an effective defence (see section 9.6).

8.4 Moreover, Intasoft observes the rights of the reported person under the General Data Protection Regulation. Reference is made to Intasoft's Privacy Policy for the Whistleblower Arrangement, which can be found at https://www.netcompany-intrasoft.com/whistleblower. The Privacy Policy contains further information on the processing of personal data and the rights of the data subject.

9 PROTECTION OF THE WHISTLEBLOWER

9.1 Whistleblowers are protected against retaliation when submitting a report to the Arrangement. Such protection only applies if the following conditions are fulfilled:

- The person submitting the report meets the conditions to be considered a whistleblower (see section 2).
- The Whistleblower had reasonable grounds to believe that the reported information was correct at the time of reporting.
- The reported information falls under the scope of violations or potential violations defined as acts or omissions (see section 3.4).

9.2 "Retaliation" means (direct or indirect) unfavourable treatment of the Whistleblower or unfavourable consequences as a reaction to a report. This may be suspension, dismissal, demotion, or equivalent measures.

9.3 If the Whistleblower submits a report in bad faith and is fully aware of the fact that the reported information is not correct, the Whistleblower is not protected against retaliation. Depending on the circumstances, the Whistleblower can be sanctioned with a fine if he or she has deliberately submitted false reports. If the Whistleblower is employed by Intrasoft, it may also have employment-related consequences, entailing inter alia the summary dismissal of the Whistleblower.

9.4 In addition to the group of persons mentioned in section 2.1, the protection described in this section 9 also applies to the following persons or entities:

1) Intermediaries

2) Third parties who are connected to the Whistleblower and who risk being subject to retaliation in a work-related context (e.g. a colleague or relative of the Whistleblower).

3) Personal businesses or legal entities of interest to the Whistleblower and authorities which the Whistleblower owns or works for or is otherwise connected with in a work-related context (e.g. an undertaking owned by the Whistleblower).

9.5 Information about the identity of the Whistleblower or any other information that directly or indirectly may reveal the Whistleblower's identity will only be disclosed to other persons than the whistleblower unit after having obtained prior explicit consent from the Whistleblower.

9.6 However, information on the Whistleblower's identity and any other information may be disclosed **without consent** only where required by EU or national law, in the context of investigations by competent authorities or in the context of judicial proceedings, and where this is necessary to serve the purposes of this Arrangement or to safeguard the rights of defence of the reported person.

9.7 Disclosures under Article 9.6 shall be made after informing the Whistleblower in writing of the reasons for the disclosure of his/her identity and other confidential information, unless such information would undermine investigations or judicial proceedings.

9.8 The identity of the Whistleblower may also be revealed in connection with legal proceedings regarding the reported matter.

9.9 If the Whistleblower has deliberately revealed his or her identity in connection with a publication of the reported matter, the special considerations regarding the protection of the Whistleblower's identity are not applicable. In such cases, information on the Whistleblower's identity may be passed on pursuant to the rules under the General Data Protection Regulation.

10 DATA SECURITY AND DATA STORAGE

10.1 Intrasoft will register all reports received under the Arrangement. Intrasoft will store a report for as long as necessary and proportionate to comply with the requirements imposed by the Whistleblowing Directive and the national Law for the protection of the Whistleblowers, and in any case until the completion of any investigation or legal proceedings initiated as a consequence of the report against the reported person, the Whistleblower or third parties.

10.2 Intrasoft and Plesner will process all information reported through the Arrangement, including information on persons reported through the Arrangement, in accordance with applicable law in force at any time.

10.3 All reports will be stored properly, and it will only be possible for relevant persons of the whistleblower unit to access the information.

10.4 A report falling outside the scope of the Arrangement will be immediately forwarded to Intrasoft's Group Legal Director and closed in the Arrangement.

10.5 In principle, reports will be deleted from the Arrangement within 45 days after Intrasoft has finalized the processing, unless Intrasoft has legitimate reasons to continue the storage, e.g. if required by other legislation, or if there is reason to believe that the report may be corroborated by subsequent reports on the same issue.

10.6 If the matter is reported to the police or another authority, the report will be closed in the Arrangement immediately after the case has been closed by the authorities in question.

10.7 If - on basis of the collected data - a disciplinary sanction is implemented against the reported person, or if there are other grounds justifying and requiring the continued storage of the data on the person concerned, such data will be stored, where an employee is involved, in the employee's personnel file.

10.8 Otherwise, the information is stored in accordance with Intrasoft's deletion policy that is included in the general Privacy Notice.

11 QUESTIONS

11.1 If you have any questions regarding this Whistleblower Policy, you are welcome to contact Tzina Prokopidou, Group Legal Director at tzina.prokopidou@netcompany-intrasoft.com or +30 6973333220.

12 UPDATING

12.1 This Whistleblower Policy has been updated on or before: *November 2022*