REPORTING GUIDE FOR WHISTLEBLOWERS

This guide presents the main aspects on the use of the ROADIS Internal Information Channel, in accordance with the regulations of the Internal Reporting System Policy and the Reporting Management Procedure. Defined terms shall have the same meaning as assigned to them in the Policy and Procedure.

ACCESS TO THE INTERNAL INFORMATION SYSTEM

1. The following persons and entities ("**Whistleblower(s)**") may make use of the Communication Channel, to the extent that they maintain some type of employment or professional relationship with ROADIS:

(i) employees, former employees, volunteers, trainees, paid or unpaid trainees; candidates in a selection processes or pre-contractual negotiation;

(ii) shareholders, participants, members of the administrative, management or supervisory body;

(iii) contractors, subcontractors, suppliers, consultants, collaborators or other persons or entities who maintain a professional relationship with ROADIS, as well as any person working for or under the supervision and direction of such persons or entities;

(iv) legal representatives of the workers in the exercise of their functions of advice and support to the Whistleblower ; and

(v) natural persons who are related to the Whistleblower and who believe that they may suffer retaliation, such as co-workers or family members of the Whistleblower.

2. Among the potential Whistleblowers, it is important to note that any person who, being an employee of ROADIS or having adhered to compliance with its Code of Conduct, has knowledge or well-founded suspicions of the commission of an event that may be reported, is obliged to report it through the corresponding Communication Channel(s).

CONTENT OF THE COMMUNICATION

The Communication addressed to the Company must contain the following information:

(i) Name and surname and personal identification document of the Whistleblower.

(ii) Company, entity or body to which the Whistleblower belongs.

(iii) Contact details (telephone, postal address, email address), for notification purposes.

If the Whistleblower wishes to make an anonymous Communication, it will not be necessary to provide the details of paragraphs (i), (ii) and (iii) above. However, you should consider the advisability of providing a method of contact that, while maintaining your anonymity, allows you to analyze the content of the Communication or request any clarification or additional information. In this sense, it is important to note that the SPEAK OUT platform allows the Whistleblower, once the Communication has been sent, to follow up on it and send additional information, even maintaining anonymity if this option was chosen.

(iv) Content of the Communication: description of the Report (events that have occurred), the entity and area of ROADIS that it affects; the date or period of occurrence of the facts; the possible Affected with knowledge, participation or responsibility in the facts.

(v) Relevant data: all relevant information available to the Whistleblower must be attached to the Communication.

FORM OF PRESENTATION OF THE COMMUNICATION

A Communication may be submitted either in writing or orally.

(i) In writing:

- Through the corporate email address: proethic@roadis.com
- Using the form available on the SPEAK OUT channel, managed by a third-party service provider (Navex), accessible online via the secure website at: http://www.roadis.ethicspoint.com

(ii) Verbally, by phone via Navex's dedicated toll-free number: +34 900-876-127

(iii) At the request of the Whistleblower, through a personal meeting. This meeting must take place within a maximum period of seven (7) days from the request for the meeting and will be attended by the Delegate of the System Manager or one of the Administrators of the IRS, if the Delegate so decides.

PROCESSING OF THE COMMUNICATION

Once a Communication has been sent, ROADIS will acknowledge receipt of it to the Whistleblower within seven (7) days, unless this may jeopardize the confidentiality of the Communication and provided that the option chosen by the Whistleblower allows it. Once received, the IRS Administrator will proceed to assign a registration number to said Communication.

The Communication shall be deemed admissible if the preliminary examination concludes that it complies with the requirements for that purpose. The System Manager will agree to this and will initiate the investigation of the facts denounced.

The Communication will be considered correctable if it suffers from any deficiency that is so and provided that the sending option chosen by the Whistleblower makes it possible, granting the System Manager a period of five (5) working days to the Whistleblower to correct it. If such deficiencies are not corrected within the aforementioned period, the Communication will be considered not made and will be inadmissible, and the file will be closed.

The Communication shall be considered inadmissible in the preliminary examination if it suffers from any deficiency that cannot be remedied, and the file shall be closed. Communications will be inadmissible in the following cases:

- When they do not refer to facts that may constitute an infringement of the Regulations.
- When sufficient information is not provided to allow a minimum verification of the facts investigated.
- When they do not present a minimum of plausibility or are manifestly unfounded.
- When there are no reasonable indications that can support the information communicated.
- When the correctable deficiencies are not corrected within the indicated period.

Whether or not to admit a Communication, this decision will be made known to the Whistleblower within five (5) business days, unless the Whistleblower is anonymous and has chosen not to provide any means of communication through which such notification can be made.

The duration of the investigation may not exceed three months from the receipt of the Communication and in cases of special complexity, this period may be extended to a maximum of three additional months.

WHISTLEBLOWER'S RIGHTS AND GUARANTEES FOR THEIR PROTECTION

The right to protection presupposes that (i) the Whistleblower has reasonably assessed that the Information is truthful at the time of the Communication, and (ii) that the Communication has been made in accordance with the formalities provided for in this Policy and in the procedures for its development.

The measures to protect the Whistleblower will consist of:

1. The prohibition of adopting any type of retaliation, negative consequence, or threat of retaliation or attempted retaliation against the Whistleblower , for the sole fact of making a Communication such as, for example:

   (i) Proceed to suspend the employment contract or terminate the employment relationship for any reason; as well as the early termination or cancellation of contracts for goods or services.

   (ii) Imposing disciplinary measures, substantially modifying working conditions, or denying labor rights.

   (iii) The imposition of the measures in paragraphs a) and b) above (or similar) will not be considered retaliation when adopted within the regular exercise of the Company's management power under labor law for reasons unrelated to the submission of the Communication by the Whistleblower .

   (iv) Causing any damage, including reputational damage, or unjustified economic loss, coercion, intimidation, harassment or ostracism.

   (v) Disseminate negative evaluations or references regarding the work or professional performance of the Whistleblower .

   (vi) Unjustifiably denying access to the training regularly provided by the Company.

   (vii) Any other form of discrimination or unfair treatment.

2. To exempt the Whistleblower from any liability arising from making a Communication, or for acquiring or accessing the Information, provided that there are reasonable grounds to believe that it was necessary to carry out such Communication in order to disclose an action or omission that violates the Regulations. This disclaimer shall not affect any criminal liability that may affect the Whistleblower as a result of his or her conduct.

   Notwithstanding the foregoing, Reporters will not be relieved of any liability incurred by them for acts or omissions that are not related to the Communication, or that were not necessary to disclose a breach. Likewise, persons who have reported or disclosed information will not enjoy the above protection measures:

   (i) That (a) lacks all plausibility; (b) does not constitute an infringement; (c) has no basis whatsoever; (d) has been obtained through the commission of a crime, or (e) does not contain new or significant information with respect to previous Communications previously received;

(ii) That the Whistleblower knew that they had already been inadmissible by some other Communication Channel for the reasons of paragraph (i) above;

(iii) Relating to interpersonal conflicts or conflicts affecting only the Whistleblower and the persons to whom the Communication relates that do not constitute a breach of the Regulations;

(iv) Public information or consisting of mere rumors;

(v) Information that does not refer to the Regulations;

(vi) False or distorted information, in bad faith or abuse of rights, may also constitute a very serious infringement of current regulations, giving rise to the appropriate disciplinary responsibilities. In addition, ROADIS reserves the right to take civil or criminal action against those responsible for such conduct.

EXTERNAL CHANNELS OF COMMUNICATION.

The main external channels of communication are the following:

(i) European Anti-Fraud Office (OLAF) https://fns.olaf.europa.eu/main_es.html

(ii) National Commission on Markets and Competition (CNMC) https://edi.cnmc.es/buzones-anonimos/sica

(iii) National Anti-Fraud Coordination Service Channel https://www.igae.pap.hacienda.gob.es/sitios/igae/esES/snca/Paginas/ComunicacionSNCA.aspx

(iv) Anti-fraud mailbox - Complaints channel of the Recovery and Resilience Mechanism https://planderecuperacion.gob.es/buzon-antifraude-canal-de-denuncias-del-mecanismo-para-la-recuperacion-y-resiliencia

(v) Municipal Office against Fraud and Corruption of Madrid https://www.madrid.es/portales/munimadrid/es/Inicio/El-Ayuntamiento/Denuncias/?vgnextfmt=default&vgnextoid=789a088847b26810VgnVCM2000001f4a900aRCRD&vgnextchannel=ce069e242ab26010VgnVCM100000dc0ca8c0RCRD&idCapitulo=11922007&rm=00369bbb53158610VgnVCM1000001d4a900aRCRD

If you need a more exhaustive list of external communication channels, as well as additional information about this guide, the Policy or the Procedure, you can contact the Compliance Officer by sending an email to complianceofficer@roadis.com