

WHAT TO REPORT

- **Conduct adopted by Saras Group people in violation of laws, the Group Code of Ethics, Organizational Model and serious violations of the provisions of the Company's Regulatory System;**
- **Breaches of Union law:**
 - **breaches falling within the scope of the Union acts set out in the Annex Directive EU 2019/1937** (that concern areas such as: (i) public procurement; (ii) financial services, products and markets, and prevention of money laundering and terrorist financing; (iii) product safety and compliance; (iv) transport safety; (v) protection of the environment; (vi) public health; (vii) protection of privacy and personal data, and (viii) security of network and information systems);
 - **breaches affecting the financial interests of the Union** (that concern for example Fraud and Bribery);
 - **breaches relating to the internal market, including breaches of 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 to arrangements the purpose of which is to obtain a tax advantage that defeats the object or purpose of the applicable corporate tax law.**
- **In Spain also actions or omissions that may constitute a serious or very serious criminal or administrative offence.**

WHAT NOT TO REPORT

- **communications relating to customer complaints, anomalies and non-conformities** that are handled within the company's management systems (e.g. quality management system) and forwarded to the relevant company departments
- **communications from investors and financial analysts** that are managed within the Investor Relations channels
- **grievances of a personal nature of the reporting person**, gossip/rumours about facts that do not constitute misconduct or violations
- **false accusations made against third parties** and, in general, deliberately inaccurate information

WHO MAY REPORT

- **persons having the status of worker, persons having self-employed status, shareholders and persons belonging to the administrative, management or supervisory body of an undertaking, including non-executive members, as well as volunteers and paid or unpaid trainees; any persons working under the supervision and direction of contractors, subcontractors and suppliers** who acquired information on breaches in a work-related context
- **persons whose work-based relationship which has since ended**
- **persons whose work-based relationship is yet to begin** in cases where information on breaches has been acquired during the recruitment process or other pre-contractual negotiations.

Anonymous reports will also be considered, and it will still be possible to be contacted via a confidential inbox.

WHAT TO INDICATE IN THE REPORT

the report must provide a sufficient degree of detail to enable the facts reported to be ascertained. The questionnaire provides a guide to be completed (we ask, where possible, to complete all fields).

MANAGEMENT OF THE REPORT

- **the reporting person can access the Inbox (of the Reporting tool) using the exclusive credentials provided at the time of reporting;** the Inbox can be used to request further information that may be used to assess the facts reported
- **the report shall be handled by the Internal Audit function** ensuring maximum **objectivity, independence and confidentiality**
- **an acknowledgement of receipt of the report will be sent to the reporting person, through the Inbox, within 7 days**
- **within three months of the acknowledgement of receipt, the results of the investigation will be sent to the reporting person, through the Inbox**

REPORTING TOOL

- **using the tool, reporting is carried out via an encrypted connection**
- **IP address and geolocation are not stored at any time.** When sending your report, you will receive your Inbox access credentials so that you can receive updates from us and communicate with us securely
- **the data you provide will be stored in a database of an independent company** that ensures high level protection of the information; all data stored in the database is encrypted using state-of-the-art technology
- **only personnel authorised to handle reports have access to the tool**

Saras Group's secure reporting system is provided by EQS Group AG. EQS Group AG is a company specialising in the management of protected whistleblowing systems. For more information see <https://www.eqs.com/>

The tool is considered a preferred channel. Alternatively, the following channels can be used:



Meeting with Head of Internal Audit Function



Postal address:

*Saras SpA Galleria Passarella 2, 20122 Milan, Italy
Attn: Head of Internal Audit Function*

External reporting channel:

Without prejudice to the preferential use of the reporting channels made available by the Saras Group, in Italy (in the cases strictly indicated pursuant to art. 6 of Legislative Decree no. 24 of 10 March 2023) and Spain, it's also possible to make reports to the competent authority (external reporting channel).

PROCESSING OF PERSONAL DATA

- **Before making a report, we ask you to consult the Privacy Policy** and confirm your acknowledgement by ticking the appropriate flag in the Reporting tool

GUARANTEED CONFIDENTIALITY AND ANONYMITY

Reports are handled in such a way as to ensure the confidentiality of the reporting person's identity, without prejudice to any legal obligations. Whistleblowers in good faith are protected against any form of retaliation, discrimination or penalisation, for reasons directly or indirectly related to the report.

The measures for the protection of reporting persons shall also apply, where relevant, to:

- **Facilitators** (means a natural person who assists a reporting person in the reporting process in a work-related context, and whose assistance should be confidential)
- **Third persons who are connected with the reporting persons** and who could suffer retaliation in a work-related context, such as **colleagues or relatives** of the reporting persons
- **Legal entities** that the reporting persons own, work for or are otherwise connected with in a work-related context
- **Anonymous whistleblowers**, if subsequently identified and subject to retaliation.

Bribery - in violation of laws and/or internal regulations, accepting money, favours or benefits from public or private persons or companies or giving money or other benefits to public or private persons or companies, in order to obtain an advantage for oneself and/or the company

Conflict of interest - accepting or granting unlawful favours, soliciting personal and career advantages for oneself or others, improperly using one's position in the company or information acquired in one's work in dealings with suppliers, customers, or other third parties for personal interests

Competition - anti-competitive practices aimed at distorting free market competition

Financial Crime - falsification, misrepresentation of information or data in company books, reports, forms or other documents used internally or externally

Fraud - misappropriation of the company's money, goods, equipment; events of unjustified shortfall or loss of materials, products, equipment, money and valuables; improper use of company materials or assets

Harassment and discrimination - physical, verbal, sexual and/or psychological harassment and abuse; discriminatory behaviour based on race, gender, nationality, political opinion, sexual orientation, social status, age and religious beliefs

International Trade Controls - violation of rules or provisions restricting or prohibiting the transfer of goods to specific countries or counterpart

Human rights and health of individuals - violation of laws, guidelines, regulations or procedures relating to workplace safety and/or human rights

Serious damage to the environment - violation of environmental laws, guidelines, regulations or procedures

Other violations of the Code of Ethics or laws and regulations - violations of National or European Union Laws, that do not fit into the above examples, that harm the public interest or the integrity of the Company; violations of Code of Ethics, Organizational Model, Policies, Regulations; serious irregularities committed as a result of violations of company guidelines, procedures; disclosure of company's confidential or inside information