SAIPEM S.p.A.
Via Luigi Russolo, 5
20138 Milano - Italia

PRIVACY NOTICE REGARDING THE PROCESSING OF PERSONAL DATA FOR THE REPORTING OF OFFENCES AND FOR WHISTLEBLOWING PURPOSES IN ACCORDANCE WITH ART. 13 AND ART. 14 OF REGULATION (UE) 2016/679 ("GDPR")

Joint Controllers

Personal data processed in the context of whistleblowing reports is processed under a joint controller agreement pursuant to article 26 of the GDPR by:

- **Saipem S.p.A.**, Via Luigi Russolo, 5 20138 Milan – Italy; e-mail: privacy@saipem.com (**"Saipem S.p.A.**");
- the subsidiary of Saipem S.p.A. that is the recipient of the whistleblowing report, whose contact details can be found on the Saipem S.p.A. website (the "**Subsidiary**") and which uses the reporting system adopted at Group level;

jointly the "**Joint Controllers**" and individually each the "**Joint Controller**".

The Joint Controllers jointly determine the purposes and means of processing personal data related to the receipt, management and investigation of reports, as well as the verification, monitoring and reporting activities required by whistleblowing legislation and Group governance models.

An essential extract from the Joint Controller agreement, which transparently governs their respective responsibilities in relation to personal data protection, is made available to data subjects upon request.

Data Protection Officer (DPO)

The DPO can be contacted at: dpo@saipem.com.

Personal Data Processed

The Subsidiary has established its own internal channels for managing reports of unlawful conduct and for ensuring the confidentiality of the identity of the whistleblower and other individuals involved, protecting them from retaliatory consequences; this process complies with the requirements of Legislative Decree no. 24/2023 "*Implementation of Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law and laying down provisions on the protection of persons who report breaches of national law*" (the "**Whistleblowing Decree**") and with the provisions set out in the Organisation, Management and Control Models pursuant to Legislative Decree no. 231/2001 and/or the Subsidiary's Organisation, Management and Control Models and in the Anti-Corruption Management System Guideline of Saipem.

The complete list of reporting channels made available by the Subsidiary is available on the Saipem S.p.A. website. Among the reporting channels available to the whistleblower, an IT platform has been set up to manage independent channels for both Saipem S.p.A. and the Saipem Group's Subsidiaries. Furthermore, in accordance with local regulations implementing Directive (EU) 2019/1937, certain companies are also required to have a Proximity Channel for subsidiaries that have employed an average of more than 249 employees in the last year.

The whistleblower is given the option of accessing the Saipem S.p.A. channel, the Subsidiary channel or, where applicable, the relevant Proximity Channel of the Subsidiary concerned. In fact, also in accordance with Directive (EU) 2019/1937, regardless of the subject matter of the report and the entity of Saipem involved, everyone is always guaranteed the possibility of sending reports directly through the Saipem S.p.A. channel, which will be handled in

compliance with and in application of the Italian whistleblowing legislation. In addition, there is a dedicated channel for reports concerning the function responsible for managing the reporting process (conflict of interest).

Pursuant to the Whistleblowing Decree, in the absence of a conflict of interest and except as provided for in relation to the proximity channel, the management of reports is entrusted to Saipem S.p.A. in its quality of data processor; pursuant to Article 4.4 of the Whistleblowing Decree, this also applies to subsidiaries.

Reports may be named or anonymous.

The personal data processed by the Controller in the context of managing the reports received is the data provided by the whistleblower in order to report the breach of which they have become aware by virtue of their legal relationship with the Subsidiary. Specifically, the personal data processed by the Joint Controllers is:

a. the whistleblower's name and surname, when the report is named;

b. additional personal data provided by the whistleblower, including special and/or judicial data, referring to i) the whistleblower; or ii) any third parties involved, such as, including but not limited to, the reported person, witnesses, facilitators.

In the cases referred to in point (a) and (b.i) above, personal data is provided directly by the whistleblower. This notice is therefore provided to the whistleblower in accordance with article 13 of the GDPR. In the cases referred to in point (b.ii) above, the personal data has not been obtained from the data subject but has been provided by whistleblower. This notice is therefore provided to the persons referred to in point (b.ii) pursuant to article 14 of the GDPR.

Please note that all the personal data provided will be processed in accordance with current legislation on privacy. Therefore, the Joint Controllers undertake to process the personal data in accordance with the principles of fairness, lawfulness and transparency, in compliance with the purposes set out below, collecting personal data only for specified and necessary purposes. Only authorised and properly trained personnel will be allowed to use the personal data in order to guarantee the necessary confidentiality of the information provided.

Purposes of the processing	Legal basis of the processing	Retention period of data
Management of reports received pursuant to the Whistleblowing Decree.	For the processing of common data, the legal basis is the legal obligation to which the Joint Controller is subject (the Whistleblowing Decree).	Personal data is retained for a period of 5 years from the date of notification of the final outcome of the reporting procedure.
	For the processing (if any) of special categories of data, the legal basis is: i) the fulfilment of obligations or the exercise of rights of the Joint Controller or the data subject in relation to labour law (pursuant to article 9, paragraph 2, letter b of the GDPR); ii) the establishment, exercise or defence of legal claims (pursuant to article 9(2)(f) of the GDPR).	
	The processing (if any) of judicial data is authorised pursuant to the Whistleblowing Decree (in	

	accordance with article 10 of the GDPR).	
The disclosure of the whistleblower's identity – or any other information from which that identity can be inferred (directly or indirectly) – to persons other than those competent to receive or follow up on reports for the following purposes: - proper management of the report; - in the context of disciplinary proceedings, if the complaint is based on the report and knowledge of the whistleblower's identity is essential for the defence of the accused.	The legal basis for the processing is the data subject's consent (pursuant to article 6(1)(a) of the GDPR).	Personal data is retained for a period of 5 years from the date of notification of the final outcome of the reporting procedure.
Documenting reports received by telephone or during a face-to-face meeting with the authorised personnel through a full transcript or minutes.		
Coordination, internal control and reporting activities at Group level, within the limits and in accordance with the procedures set out in the organisational model adopted.	The legal basis for the processing is the legal obligation to which the Joint Controller is subject (Whistleblowing Decree).	
If necessary, to assert or defend the right of the Joint Controller in court or in arbitration and conciliation procedures.	The lawfulness of processing is based on the Joint Controller's legitimate interest in protecting its rights (art. 6, par. 1 lett. f) e art. 9, par. 2, lett. f) of the GDPR).	For the entire duration of the legal disputes, until completion of the terms of implementation outlined in legal remedies.
Once the above retention periods have expired, personal data will be anonymised, in accordance with the timeframes set out in the technical procedures for deletion and backup.		

Methods of Processing and Provision of Data

Depending on the method chosen by the whistleblower for reporting, the processing will be carried out in digital, paper or oral form, using methods and tools designed to ensure maximum security and confidentiality, by persons specifically appointed for this purpose.

The provision of the whistleblower's personal data is optional; whistleblowers who do not wish to disclose their personal data may submit an anonymous report.

SAIPEM S.p.A.
Via Luigi Russolo, 5
20138 Milano - Italia

Recipients and Data transfer

Within the purposes listed above, personal data may be disclosed to third parties perfoming outsourced activities on behalf of the Joint Controllers, such as the suppliers of the IT platform used for the submission and management of reports or any third parties entrusted with the management of the reporting channel on behalf of the Subsidiary – in their capacity as data processors under art. 28 GDPR, as well as to third parties acting as autonomous data controller, including but not limited to the judicial Authorities.

These entities are required to comply with the data protection obligations and implement appropriate technical and organizational measures to ensure the confidentiality and security of the data.

To find out the complete and updated list of data processors appointed by the Joint Controllers, the data subject can submit a request using the contact details provided by the Controller.

Transfer of data to countries outside the European Economic Area

Personal data described in the notice is not transferred outside the European Economic Area.

Data subjects' rights

Data Subjects have the right to request from the Joint Controllers access to their personal data, as well as rectification, erasure, restriction and objection to processing within the limit provided by the GDPR. Given the nature of the processing, the right to portability cannot be exercised. Furthermore, where applicable, data subjects may withdraw their consent at any time. Withdrawal shall not affect the lawfulness of processing based on consent before its withdrawal.

These rights can be exercised at any time by submitting a written request at the following e-mail addresses dpo@saipem.com or privacy@saipem.com.

Data Subjects have also the right to lodge a complaint to the competent Supervisory Authority and to use other means of protection provided by applicable law.

Pursuant to article 2-undecies of Legislative Decree no. 196/2003 (hereinafter, the "**Code**"), the rights referred to in articles 15 to 22 of the GDPR cannot be exercised if the exercise of such rights could result in actual and concrete prejudice to the confidentiality of the identity of the whistleblower who reports unlawful conduct, pursuant to the Whistleblowing Decree, of which they have become aware.

In such cases, the rights in question may be exercised through the Data Protection Authority in accordance with the procedures set out in Article 160 of the Code.