







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

 <p><b>Data Controller</b></p> <p>The data provided are processed by <b>Saipem S.p.A.</b>, Via Luigi Russolo, 5 20138 Milan - Italy.        E-mail address: <a href="mailto:privacy@saipem.com">privacy@saipem.com</a> ("Company" or "Controller")</p>	 <p><b>Data Protection Officer (DPO)</b></p> <p>The DPO can be contacted at: <a href="mailto:dpo@saipem.com">dpo@saipem.com</a></p>		
 <p><b>Personal Data Processed</b></p> <p>The Company allows reporting issues relating to the internal control system, corporate reporting, corporate administrative liability, fraud or other matters (e.g. Code of Conduct violations, mobbing, theft, security), hereinafter "Model 231 - Including the Code of Ethics", by sending a message to the Company's e-mail address, using the reporting form on the Company's website, by ordinary mail or through the dedicated telephone line channel.</p> <p>Reports may be <b>nominal</b> or <b>anonymous</b>.</p> <p>The whistleblower may indicate his/her personal data, in case of nominal reports (e.g. personal details), as well as personal data (common data, special categories of data and/or judicial data) of the reported person and/or of any third parties.</p> <p>Please note that all the personal data provided will be processed in accordance with current privacy legislation. Therefore, the Company undertakes to process said data in accordance with the principles of fairness, lawfulness and transparency, in compliance with the purposes set out below, collecting them to the extent necessary and accurate for processing. Only authorised and properly trained personnel will be allowed to use said data in order to guarantee the necessary confidentiality of the information provided.</p>			
 <p><b>Purposes of the processing</b></p>	 <p><b>Legal basis of the processing</b></p>	 <p><b>Retention period of data</b></p>	
<p>1. Managing of reporting issues relating to the internal control system, corporate reporting, corporate administrative liability, fraud or other matters (e.g. Code of Conduct violations, mobbing, theft, security, ecc.)</p>	<p>The lawfulness of the processing for common data is based on the need to comply with the legal obligations to which the Controller is subject. With regard to special categories of data to fulfil the obligations or to exercise the rights of the Controller or data subject in the field of labor law (art. 9.2, lett. b) GDPR). The lawfulness of processing for data relating to criminal convictions and offences is the compliance with the Provisions of Model 231 (including the Code of Ethics).</p>	<p>Personal data are kept for a period of 5 years from the date of notification of the final outcome of the reporting procedure.</p>	
<p>2. To assert or defend a right of the Company in court or in arbitration</p>	<p>The lawfulness of processing for common data is the legitimate</p>	<p>For the duration of any legal disputes until completion of the</p>	

and conciliation procedures in the cases provided for by law, by European Union law, where necessary.	interest of the Data Controller. With regard to special categories of data the lawfulness of processing is to establish, exercise or defend the rights in court pursuant to art. 9. paragraph 2, lett. f) of GDPR.	terms of implementation outlined in legal remedies.
---	--	---

Once the retention period has elapsed the data will be destroyed or made anonymous compatibly with technical erasure and backup procedures.



### Way of processing and provision of data

The processing will be carried out digitally, on paper or orally, in ways and means designed to ensure ensuring maximum security and confidentiality, by persons specifically appointed for this purpose.

Completion of the fields marked with an asterisk (\*) on the form on the institutional website is mandatory and failure to complete them will make it impossible to continue the reporting process.

The provision of the whistleblower's personal data is optional; the report will be anonymized if they are not provided.



### Recipients and data transfer

The Company - without needing specific consent - may communicate personal data to other subjects, the categories of which are described in detail below, for example:

- Saipem Group companies, even if not located in the EU (based on the adequacy decisions by the European Commission or on the basis of standard contractual clauses);
- Third parties (by way of indication, companies providing IT services, etc.), including those not located within the EU, who carry out outsourcing activities on behalf of the Controller, in their capacity as data processors. The transfer of data to countries outside the EU is guaranteed by the adequacy decisions of the European Commission or on the basis of standard contractual clauses;
- Judicial authorities, insurance companies for the provision of insurance services, as well as those subjects to whom communication is required by law or by contract. These subjects will process the data in their capacity as independent Data Controllers.

Your data will not be subject to disclosure.



### Data Subjects rights

Data Subjects have the right to ask the Controller for access to their personal data, rectification, deletion or portability of their personal data, integration of incomplete personal data, limitation of processing in the cases provided for by art. 18 GDPR. In addition, where applicable, Data Subjects may revoke their consent at any time.

These rights can be exercised at any time, against the Controller, by sending a specific request in writing to the e-mail addresses [dpo@saipem.com](mailto:dpo@saipem.com) or [privacy@saipem.com](mailto: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, as amended by Legislative Decree no. 101/2018 (hereinafter, the "Code"), the rights referred to in GDPR Articles 15 to 22 may not be exercised if the exercise of such rights may result in actual and concrete prejudice to the confidentiality of the identity of the whistleblower who reports unlawful conduct, pursuant to Law no. 179/2017, of which he/she has become aware.

In such a case, the rights in question may be exercised through the Supervisory Authority (as set out in Article 160 of the Code), who shall inform the data subject that he/she has carried out all the necessary verifications or



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

	has carried out a review, as well as of the data subject's right to seek judicial redress.
--	--