







**INFORMATION NOTICE REGARDING THE PROCESSING OF VENDORS' PERSONAL DATA
 FOR THE STIPULATION AND EXECUTION OF CONTRACTS
 IN ACCORDANCE WITH ARTT. 13 AND 14 OF REGULATION (UE) 2016/679 ("GDPR")**

 <p>Data Controller</p> <p>The data provided are processed by Saipem S.p.A., Via Luigi Russolo, 5 20138 Milan - Italy. E-mail address: privacy@saipem.com ("Company" or "Controller")</p>	 <p>Data Protection Officer (DPO)</p> <p>The DPO can be contacted at: dpo@saipem.com</p>	
 <p>Personal Data Processed and source of data</p> <p>Please note that all the personal data provided will be processed in accordance with current legislation on privacy. 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 said data only for specified and necessary purposes. 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>In particular, the Company will collect, record, consult and generally process the personal data of the legal representative, directors and, if necessary, their family members, supplier's employees and associate with which the Company intends to enter into the contract. Specifically, the personal data processed by the Controller will be the common data (e.g. name, surname, address, telephone, e-mail, or in any case personal data available on public sources).</p> <p>Personal data may be collected from the counterparty or from third party specialised in providing this data (info provider).</p>		
 <p>Purpose of the processing</p>	 <p>Legal basis of the processing</p>	 <p>Retention period of data</p>
<p>1. Execution of the due diligence activities, preliminary to the establishment of a contractual relationship (for example, carrying out preliminary assessments, adding, updating, or monitoring of the registry).</p>	<p>The lawfulness of processing for the common data is the execution of pre-contractual measures. If necessary, the processing of judicial data is for Company's compliance with the requirement of Model 231 (including the Code of Ethics).</p>	<p>Personal data will be stored for 10 years after the assignment of the contract and any due diligence process with the supplier, except for the need to extend the retention period for the duration of any litigation until completion of the terms of implementation outlined in legal remedies.</p>
<p>2. Management of contractual relations with suppliers.</p>	<p>The lawfulness of processing for the personal data is the execution of a contract to which the data subject is a party.</p>	
<p>3. Comply with statutory provisions (for example: anti-money laundering, safety and health in the workplace).</p>	<p>The lawfulness of the processing is based on the need to comply with the legal obligations to which the Controller is subject.</p>	

4. IT security management, including log file management to detect malicious access and behaviour.	The lawfulness of the processing is the legitimate interest of the Data Controller in protecting the security of the company's information assets.	Personal data will be kept only as long as strictly necessary to fulfill the purpose. With regard to the management of logs, a retention period of 6 months from their registration.
5. Data mining activities to improve work processes.	The lawfulness of processing for common data is the legitimate interest of the Data Controller in optimising operational processes according to a data-driven logic on the use of data for business decisions.	Personal data will be kept only as long as strictly necessary to fulfill the purpose.
6. If necessary, to assert or defend a right of the Company in court or in arbitration and conciliation procedures.	The lawfulness of processing for common data is the legitimate interest of the Data Controller.	For the duration of any legal disputes until completion of the 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 in digital and/or traditional form, with methods and tools aimed at ensuring maximum security and confidentiality, by persons specifically appointed for this purpose.

The processing of the above-mentioned data is necessary for the execution of the contract and for the fulfilment of legal obligations; therefore, your refusal will make impossible the establishment of the contractual relationship.



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), in order to carry out contract management activities;
- Third parties (by way of indication, companies providing IT services), 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;



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 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.

- Judicial authorities, as well as those subjects to whom communication is required by law. These subjects will process the data in their capacity as independent Data Controllers.

Data will not be subject to disclosure.