

**PRIVACY NOTICE ON THE PROCESSING OF PERSONAL DATA FOR JOB APPLICANTS
PURSUANT TO ARTICLES 13 AND 14 OF REGULATION (EU) 2016/679 ("GDPR")**

 Data Controller Saipem S.p.A., Via Luigi Russolo, 5 20138 Milan – Italy, E-mail address: privacy@saipem.com (“Company” or “Controller”) acts as the data controller for the processing of your personal data.	 Data Protection Officer (DPO) The DPO can be contacted at:dpo@saipem.com	
 Personal data processed and source of data Please note that your personal data will be processed in compliance with applicable data protection laws. Therefore, the Company processes personal data in accordance with the principles of fairness, lawfulness and transparency, in compliance with the purposes set out below, collecting only the personal data necessary for the specific purposes described below. Only authorised personnel who have received appropriate training may access such data in order to guarantee the necessary confidentiality of the information provided. The Company processes the personal data you provide when submitting a voluntary application or responding to job advertisements published by the Company or by third parties, such as recruitment agencies. Specifically, the Company processes: - standard personal data, such as personal details, contact details, and information relating to education and professional experience (for example, first name, surname, tax number, gender, place and date of birth, telephone number, e-mail address; nationality, educational qualifications, IT and language skills), as well as any other data you have voluntarily included in your CV; - the following personal data belonging to special categories that you may have provided during the application process: information relevant to equal employment opportunity requirements, and, in the final stage of the selection process, suitability to perform the role for which you are applying; - in the final stage of the selection process, for applications relating to specific roles deemed particularly sensitive or high-risk, data relating to criminal convictions and offences, limited to those relevant to the role to be performed, as well as, where necessary, for the purposes of obtaining visas, permits or other authorisations required for travel to the destination country. Data is collected directly from the data subject and/or from third parties, such as recruitment agencies.		
 Purposes of processing	 Legal bases for processing	 Retention period
1. Recruitment and selection of personnel.	The legal basis for the processing of general data is the implementation of pre-contractual measures taken at your request (Article 6.1(b) of the GDPR). For special categories of data, the need to comply with obligations or exercise rights under applicable labour law (pursuant to Article 9.2(b) of the GDPR) and the need to assess suitability for the role for which	Personal data will be retained for 12 months from the date of submission of your application, unless further retention is required for the purposes set out below.

	you are applying pursuant to Article 9.2(h) of the GDPR. The processing of criminal records is authorised pursuant to Legislative Decree 231/2001 (in accordance with Article 10 of the GDPR).	
2. Retention of information relating to the job applicant for the purpose of assessing their profile with a view to possible future career opportunities.	The legal basis for the processing is the data subject's consent pursuant to Article 6.1(a) of the GDPR and Article 9.2(h) of the GDPR.	Personal data will be retained for 12 months from the date on which the data subject gave their consent to the retention of their personal data.
3. Sending communications regarding further career opportunities deemed to be consistent with the job applicant's profile and inviting them to submit an application.		Personal data will be retained for 12 months from the date the application was submitted or from the moment the data subject gave their consent to the retention of their personal data.
4. Documentation and traceability of the recruitment process for the purposes of improving the efficiency of future recruitment processes, carrying out audits and internal controls, and managing any reports.	The legal basis for the processing of general data is the Data Controller's legitimate interest in ensuring the proper management, traceability and verifiability of the recruitment process (Article 6.1(f) of the GDPR).	Data relating to the management of the recruitment process will be retained for 5 years from the conclusion of the recruitment process. Please note that not all data relating to the application will be retained, but only that necessary to document and track the management of the recruitment process, such as the job applicant's identity, the date the application was submitted, the internal personnel involved in the assessment, the results of the assessments carried out and the reasons underlying the final decision taken.
4. Where necessary, to establish, exercise and/or defend the Company's rights in judicial, administrative or arbitration and conciliation proceedings.	The legal basis for the processing of general personal data is the Data Controller's legitimate interest. The legal basis for the processing of special categories of personal data is the establishment, exercise or defence of a legal claim, in accordance with Article 9.2(f) of the GDPR.	For the duration of the relevant proceedings and thereafter for as long as necessary to enforce or comply with any resulting judgment, settlement or other legal remedy.
Once the above retention periods have expired, personal data will be deleted or made anonymous compatibly with technical erasure and backup procedures.		



Way of data processing and provision of data

The processing will be carried out in digital form, with appropriate security and confidentiality measures by personnel specifically authorised and trained for this purpose, while also ensuring an adequate level of accuracy, resilience and cybersecurity of the systems, in line with applicable best practices and industry standards.

In the case of an online application, via the portal on the Company's website, the provision of data marked with an asterisk (*) is necessary for your application to be considered as part of the recruitment and selection process. Failure to provide this data will prevent this process from taking place and, consequently, your application cannot be considered.



Recipients and data transfer

Within the purposes listed above, personal data may be disclosed to third parties performing outsourced activities on behalf of the Controller – including but not limited to IT service providers and recruitment platforms, companies supporting the recruitment process, companies within the Saipem Group, consultants and other parties involved in the management of staff recruitment, selection and hiring activities – 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 competent Authorities and clients.

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 Data Controller, the data subject can submit a request using the contact details provided by the Data Controller.



The rights of the data subject

Data Subjects have the right to request from the Controller access to their personal data, rectification, deletion, portability, restriction and objection to processing, as provided for by the GDPR.

Furthermore, where applicable, data subjects may withdraw their consent at any time. Such withdrawal shall not affect the lawfulness of processing based on consent prior to its withdrawal.

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.



Transfer of data to countries outside the European Economic Area

The personal data processed is not transferred outside the European Economic Area.

Should it become necessary, for purposes related to the above-mentioned purposes, to transfer personal data to countries located outside the EEA, such transfers will be carried out in compliance with the GDPR and, in particular, on the basis of an adequacy decision adopted by the European Commission or through the implementation of the Standard Contractual Clauses approved by the European Commission, or other appropriate safeguards provided for under applicable law.