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

PRIVACY NOTICE REGARDING THE PROCESSING OF PERSONAL DATA OF EMPLOYEES AND INDIVIDUALS WHO, FOR VARIOUS REASONS, ACCESS CRITICAL WORKPLACES, PURSUANT TO ART. 13 OF REGULATION (EU) 2016/679 ("GDPR") AND THE USE OF ARTIFICIAL INTELLIGENCE SYSTEMS PURSUANT TO REGULATION (EU) 2024/1689 ("AI ACT")

Data Controller and *deployer*

The data controller pursuant to the GDPR and deployer pursuant to the AI Act is:

Saipem S.p.A., Via Luigi Russolo, 5 20138 Milan - Italy.

E-mail address: privacy@saipem.com ("**Company**" or "**Controller**").

Data Protection Officer (DPO)

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

Video Analytics System

The Video Analytics System (the "**VAS**") is a video analysis system supporting Health, Safety and Environment (HSE) supervision used for the progressive identification of unsafe conditions and/or acts in the workplace. It works through image and video streams transmitted to locally installed software, which can only be accessed by specifically authorised and trained individuals.

The VAS is able to identify a limited set of unsafe acts and/or conditions and sends real-time notifications to authorised individuals, thanks to Artificial Intelligence ("**AI**") technology, in order to improve safety in critical workplaces. Once the notification is received, authorised individuals immediately take action to verify the accuracy of the report and manage the event that generated it. At the end of the event, anonymised reports on the events that occurred may be issued.

The VAS is a field supervision support system, without the aim of altering, replacing or reducing normal activities, responsibilities and coordination rules.

Provision of data, how the VAS works and AI

Personal data is collected by cameras that transmit to:

- a Network Video Recorder ("**NVR**"), a traditional video surveillance system that supports the VAS and transmits and records the video stream in real time in non-anonymised video format;
- the VAS, which produces anonymised frames when unsafe acts and/or conditions are detected.

The VAS consists of cameras equipped with an application that uses artificial intelligence technology to report, in real time, to authorised persons, any behaviour that does not comply with the standards set for the protection of health and safety in the workplace. It should be noted that any decision or action resulting from a reported event is always subject to human verification (known as "human in the loop").

To enable the automatic security anomaly detection system to function, a predefined AI model (known as out-of-the-box training) is used, which is provided by the manufacturer and not customised. Only if it becomes necessary to improve this algorithm (e.g. in the case of numerous false positive notifications) will training be carried out using data collected by the cameras exclusively for the purpose of improving the VAS system itself. The data will not be used in any way to train other algorithms or third-party systems. The use of data to improve the algorithm is carried out in a non-anonymised form; once the training phase is complete, this data is not stored further.

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

Personal Data Processed

Please note that all the personal data collected by the cameras will be processed in accordance with current legislation on privacy. Therefore, the Company undertakes 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.

In particular, the Company processes the following personal data collected from the data subject: images (still images) and videos (without audio) captured by cameras.

Purposes of the processing	Legal basis of the processing	Retention period of data
Workplace safety to protect the safety of workers and those who, for various reasons, frequent critical workplaces.	The legal basis for the processing of personal data is the legitimate interest of the Data Controller, pursuant to Article 6(1)(f) of the GDPR, in order to ensure a high level of safety in critical workplaces to protect the life and physical integrity of workers and those who, for various reasons, frequent critical workplaces. This interest has been subject to a specific legitimate interest assessment (LIA) with the rights and freedoms of the data subjects, ensuring that the system is configured to minimise the impact on the privacy of workers. The lawfulness of processing employees' personal data is also subject to compliance with article 114 of Legislative Decree 196/2003 ("*Codice Privacy*"), article 26.7 of the AI Act and article 4 of Law 300/1970 ("*Statuto dei Lavoratori*"), given the conclusion of an agreement with trade union representatives.	The images are immediately anonymised in an irreversible manner and deleted within **24 hours** of their creation. The videos are stored for **24 hours** from the time the images are captured, after which the data is automatically deleted by overwriting.
In the event of an incident that generates notifications, where necessary for internal analysis and investigations relating to the reported events (including but not limited to reconstruction of the dynamics of accidents, injuries or near misses).		The frames and videos relating to events that have generated notifications are stored for the time strictly necessary to conduct internal analyses and investigations, and in any case no longer than the closure of the relevant incident report, unless further storage is necessary for legal purposes.
If it is necessary to improve the algorithm, the data collected by the cameras will be used to train the system's artificial intelligence algorithm.		For the time strictly necessary to improve the algorithm only.
If necessary, to assert or defend the right of the Company in court or in arbitration and conciliation procedures.	The lawfulness of processing is based on the Data Controller's legitimate interest in protecting its rights in accordance with art. 6, par. 1, lett. f) 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 automatically deleted or overwritten.

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

Way of processing

The processing will be carried out digitally, using methods and tools designed to ensure maximum security and confidentiality, by persons specifically appointed for this purpose, as well as an adequate level of accuracy, robustness and cybersecurity of the systems in accordance with the best reference standards

Recipients and Data transfer

Within the purposes listed above, personal data may be disclosed to third parties perfoming outsourced activities on behalf of the Controller – including but not limited to companies that supply the cameras and the VAS or that perform system maintenance – 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 competent Authorites.

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.

Data subjects' rights

Data Subjects have the right to request from the Controller access to their personal data, as well as erasure and restriction to processing in the cases provided for by GDPR.

In view of the objective nature of the images captured, the right to rectification cannot be exercised with regard to the video content. Furthermore, the conditions for exercising the right to data portability pursuant to article 20 of the GDPR do not exist, as the processing is not based on consent or a contract, but on the legitimate interest of the Data Controller.

Please note that, for the processing activities based on legitimate interest, the right to object cannot be exercised since the legitimate interest pursued by the Controller prevails, while respecting the interests, rights, and freedoms of the data subjects.

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.

Transfer of data to countries outside the European Economic Area

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

Only in exceptional cases, subject to specific authorisation, may the software provider based in the United Kingdom have access to the data for the sole purpose of resolving any technical problems. The European Commission has recognised the United Kingdom as providing an adequate level of data protection through an adequacy decision; therefore, no further measures are necessary for this possible transfer of personal data.

Any transfer of personal data outside the EEA by the supplier is entirely residual. If necessary for the performance of the contract, the supplier will take appropriate safeguards, such as Standard Contractual Clauses (SCCs), as provided for in the contractual provisions.