
	Saudi Arabian Saipem Co Ltd		Doc. no. FORM-SAS-PRV-001-E
	INFORMATION REGARDING THE PROCESSING OF PERSONAL DATA FOR VISITORS PURSUANT TO Article 13 of the Personal Data Protection Law (PDPL), Article 4 of the PDPL Implementing Regulations and Articles 13, 14 of EU REG. 2016/679 ("GDPR")		Rev. 01
			Date 29/08/2024
	Page 1 of 4		Doc. Ref. STD_GR-GROUP-PRV-001-I






INFORMATIVE CONCERNING THE PROCESSING OF IMAGES COLLECTED VIA SMART CAMERA AT CRITICAL WORKPLACES

**Article 13 of the Personal Data Protection Law (PDPL), Article 4 of the
PDPL Implementing Regulations and Articles 13, 14 of EU REG.
2016/679 ("GDPR")**

Hereby, in accordance with the provisions of Article 13 of the Personal Data Protection Law (PDPL), Article 4 of the PDPL Implementing Regulations and Articles 13 and 14 of the GDPR, we provide information regarding the processing of personal data acquired and processed through the video surveillance system operating on board of vessel "Perro Negro".

INFORMATION REGARDING THE PROCESSING OF PERSONAL DATA OF WORKERS AND SUBJECTS WHO FOR VARIOUS PURPOSES FREQUENTLY ATTEND CRITICAL WORKPLACES, PURSUANT TO ARTICLE 13 OF THE PERSONAL DATA PROTECTION LAW (PDPL), AND ARTICLE 4 OF THE PDPL IMPLEMENTING REGULATIONS


Data controller
 The data you provide are processed by Saudi Arabian Saipem Co Ltd
 E-mail: privacysas@saipem.com ("Company" or "Data controller")

<div>  Personal Data </div>	<div>  Purposes of processing </div>	<div>  Legal basis of processing </div>	<div>  Retention period </div>
Common personal data (images collected by the video surveillance system)	Guarantee the health and safety of workers and of whom, in various capacities, attend critical workplaces	The legal basis that legitimizes the processing of personal data for the stated purposes is the legitimate interest of the Data Controller, pursuant to Art. 6(1)(f) GDPR and Art. 6(4) PDPL, in order to ensure a high level of safety in critical workplaces to protect the lives and physical integrity of workers and of whom, in various capacities, attend critical workplaces. If the personal data are not collected, the data controller may not be able to prevent or respond to potential accidents, which may have serious consequences for the health and safety of the data subjects and others.	24 hours after image detection
	Analysis and internal investigation related to the events reported by the video surveillance system in terms of safety at critical workplaces		in case of "safe/unsafe" report, anonymized frames detected by video surveillance cameras shall be retained for 30 days
	Training of artificial intelligence algorithm to allow unsafety conditions detection	Legitimate interest of the data controller consisting in the right to judicial protection	3 months after image detection
	If necessary, exercise of the Company's rights in judicial, administrative, or conciliation procedures.		Throughout the duration of the litigation, until the time limits for appeal actions are exhausted.
After the above retention periods have expired, personal data will be subject to automatic deletion.			
<div>  Mode of operation and security of video surveillance systems and how the data is processed The video surveillance system consists of cameras equipped with an application that exploits artificial intelligence technology, which makes it possible to report, in real time, to the person in charge of safety, behaviors, held by employees, that do not comply with the standards placed to protect health and safety in the workplace. The personal data thus collected are anonymized upon receipt of the images and in any case within a minimum time frame. </div>			

In order to enable the operation of the automatic safety anomaly recognition system, a model is prepared using training elements constituting images (e.g., with squares drawn on the safety harness so that the model can learn to recognize the same harness). Once trained, the model will be validated against a new, previously unused dataset to evaluate its performance.

Processing will be carried out in digital and/or paper form, with methods and tools designed to ensure maximum security and confidentiality, by individuals specifically appointed for this purpose, as well as an adequate level of accuracy, robustness, and cybersecurity of the systems in accordance with the best practice.

All personal data will be processed in accordance with current privacy regulations. Therefore, the data controller undertakes to process them in accordance with principles of correctness, lawfulness, transparency, only in accordance with the stated purposes, collecting them to the extent necessary and exact for processing, allowing their use only by personnel authorized and trained for the purpose and in order to ensure the necessary confidentiality of the information provided.

The systems implemented do not make any decisions based solely on automated processing of personal data, but only provide alerts and suggestions to the person in charge of safety, who is responsible for verifying and evaluating the situation and taking any appropriate action.

The collection of personal data is done directly through the data subject or by proxy given to the delegate, if any.



Communication and outreach

The Company - without the need to request your specific consent - may communicate your personal data to categories of entities detailed below such as:

- third parties (by way of example, companies providing IT services, companies offering reception and concierge services, companies performing maintenance of video surveillance systems), which perform outsourced activities on behalf of the Data Controller, in their capacity as data controllers and are required to comply with obligations regarding the protection of personal data and the application of special technical and organizational measures to guarantee the confidentiality and security of the data;
- Judicial Authority. This will process the data in their capacity as autonomous data controllers.

The data processed will not be subject to dissemination.



Transfer of data to countries outside your country

The personal data processed is transferred outside the European Union or the Kingdom of Saudi Arabia, as applicable, in accordance with the *Standard Contractual Clauses* published by the European Commission in Implementing Decision No. 2021/914 and Article 46 GDPR, as well as Article 5 of the PDPL Transfer Regulations.



The rights of the data subject and right to complain

The data subject has the right to request from the Data Controller access to personal data concerning him/her, their rectification, erasure, opposition to processing as well as the integration of incomplete personal data and the restriction of processing in the cases provided for in Article 18 GDPR and Article 7(1) PDPL.

With reference to the recorded images, in accordance with the Provision of the Guarantor for the Protection of Personal Data regarding video surveillance, the right to update or supplement, as well as the right to rectification is not exercisable in practice in view of the intrinsic nature of the data processed.

These rights may be exercised at any time against the Holder by sending a request in writing to privacysas@saipem.com

In addition, he/she has the right to lodge a complaint with the Data Protection Authority and have recourse to the other remedies provided by the applicable legislation.