







| | | | |
|---|--|--|-----------------------------|
|  | FORM of Saipem Luxembourg | | Doc. n. FORM-SLUX-PRV-001-E |
| | INFORMATION NOTICE ON THE PROCESSING OF IMAGES COLLECTED VIA OPTICAL CAMERAS WHEN UNAUTHORIZED PERSONNEL ACCESS RED ZONES PURSUANT TO ARTICLE 13 OF REGULATION (EU) 2016/679 ("GDPR") | | Rev. 01 |
| | | | Date 07/04/2025 |
| | | | Page 1 of 3 |
| | Doc. Ref. STD_GR-GROUP-PRV-001-E | | |





INFORMATION NOTICE CONCERNING THE PROCESSING OF IMAGES COLLECTED VIA OPTICAL CAMERA WHEN UNAUTHORIZED PERSONNEL ACCESS RED ZONES

(Article 13 REG. (EU) 2016/679 ("GDPR"))

Hereby, in accordance with the provisions of Article 13 of the GDPR, we provide information regarding the processing of personal data collected and processed through the video surveillance system operating on Saipem 12000

**INFORMATION NOTICE CONCERNING THE PROCESSING OF IMAGES COLLECTED VIA OPTICAL CAMERAS WHEN
UNAUTHORIZED PERSONNEL ACCESS RED ZONES PURSUANT TO ART. 13 OF THE REGULATION (EU) 2016/679 ("GDPR")**

|  Data controller <p>SAIPEM LUXEMBOURG S.A. (hereinafter referred to as the "Company" or the "Data Controller") is the data controller of the personal data collected through optical cameras and processed in accordance with the GDPR, and applicable data protection laws, as set forth below.</p> <p>The Company is available at the following e-mail address: privacy.slux@saipem.com.</p> | | | |
|--|--|---|---|
|  Personal Data |  Purposes of the processing |  Legal basis of the processing |  Retention period |
| Images collected by the video surveillance system | Ensure the health and safety of workers and of those whom, in various capacities, attend critical workplaces. | The legal basis of the processing is the legitimate interest of the Company pursuant to Art. 6(1)(f) GDPR, in particular, to ensure a high level of health and safety in critical workplaces and to protect the lives and physical integrity of workers and of those whom, in various capacities, attend critical workplaces. | The images are collected in real-time, but the related recording and storage are only implemented if unauthorized access is detected. In such cases, the images are stored for 72 hours, unless necessary for the additional purposes outlined here. In any case, upon expiration of the indicated storage time, the images are subject to automatic deletion. |
| | Analysis and internal investigation of images reporting unauthorized access to critical workplaces and behaviors found non-compliant with internal procedures and rules on health and safety in the working context. | | In the event of the need to investigate an incident arising from the activation of the alert system and the report of unauthorized access, anonymized frames detected and recorded are retained for the time necessary to complete the investigation and in any case up to [7 days]. In any case, upon expiration of the indicated storage time, the images are subject to automatic deletion. |
| | Compliance with specific requests from the judicial authority or the law enforcement authorities in relation to investigations. | The legal basis of the processing is the necessity to comply with a legal obligation to which the controller is subject pursuant to Art. 6(1)(c) GDPR. | In case of a specific request from the judicial authority or the law enforcement authorities in relation to investigations, the images can be retained for the time necessary to comply with such request. |

| | | | |
|---|---|--|--|
| | Exercise of the Company's right of defence. | The legal basis of the processing is the legitimate interest of the Company pursuant to Art. 6(1)(f) GDPR, in particular, to the exercise of the right to defence. | The images are retained throughout the duration of the litigation and in accordance with the statutes of limitations with reference to torts of a contractual/tort nature. |
| <div></div> <h3>How personal data are processed</h3> <p>The video surveillance system consists of optical field cameras with machine vision technology which is able to detect any unauthorized person not equipped with the specific wearable device which authorizes entering a red zone. When this happens cameras trigger an alarm, which reports, in real time, to the person in charge of safety that an unauthorized person violated a red zone</p> <p>Processing is carried out in digital and/or paper form, with methods and tools designed to ensure maximum security and confidentiality, by individuals specifically and duly authorized and instructed for this purpose, as well as an adequate level of accuracy, robustness, and cybersecurity of the systems in accordance with the best practices.</p> | | | |
| <div></div> <h3>Recipients of personal data</h3> <p>The Company may communicate the personal data to the following categories of subjects detailed below, such as:</p> <ul style="list-style-type: none">third parties (by way of example, companies providing IT services, companies offering reception and concierge services, companies performing maintenance of video surveillance systems);judicial and law enforcement authorities. | | <div></div> <h3>The rights of the data subject</h3> <p>The data subject has the right to request from the Company access to personal data concerning him/her, their rectification, erasure, portability, opposition to processing as well as the integration of incomplete personal data and the restriction of processing in accordance with the GDPR.</p> <p>These rights may be exercised at any time against the Holder by sending a request in writing to privacy.slux@saipem.com.</p> <p>In addition to the above, the data subject has the right to lodge a complaint with the Data Protection Authority.</p> | |
| <div></div> <h3>Transfers of personal data to third countries</h3> <p>The personal data are transferred outside the European Union and, in particular, to the UK, in presence of an adequacy decision by the European Commission.</p> | | | |
| <h3>Nature of provision of personal data</h3> <p>The provision of personal data is not mandatory since they are automatically collected only if the data subjects enter a red zone as an unauthorized person not equipped with the specific wearable device which authorizes entering a red zone.</p> | | | |
| <h3>Availability of this information notice</h3> <p>This notice is made available also on Saipem website at www.saipem.com.</p> | | | |