

**INFORMATION NOTICE REGARDING VIDEO SURVEILLANCE
IN ACCORDANCE WITH ART. 13 OF THE EUROPEAN REGULATION 2016/679 ("GDPR")**



DATA CONTROLLER

The Data Controller is **S.A.C.B.O. S.p.A.**, based in Via Orio al Serio 49/51 - 24050 Grassobbio (BG), which can be contacted at the e-mail address privacy@sacbo.it



DATA PROTECTION OFFICER (DPO)

The Data Controller has appointed a Data Protection Officer (DPO), identifiable as the **Partners4Innovation** Company, who can be contacted at the e-mail address dpo@sacbo.it



OBJECT OF THE INFORMATION NOTICE

S.A.C.B.O. S.p.A. (hereinafter also the "Company") informs that a closed-circuit video surveillance system is in operation at the airport and the airport grounds. This system is appropriately signaled before its range of action by specific signs as provided for in the "Provvedimento Generale per la Protezione dei dati personali sulla Videosorveglianza" of the Italian Privacy Authority and in the "Guidelines 3/2019 on processing of personal data through video devices" (hereinafter "Guidelines") of the European Data Protection Board ("EDPB").

The cameras are installed outside and inside the airport and the airport grounds.

S.A.C.B.O. S.p.A. also reports that some cameras are installed on request and as needed, or in any case directly managed, both by the Police or other Authorities and by the Airport Manager.



SIGNALS OF CCTV CAMERAS and PROCESSING OF PERSONAL DATA

The video surveillance areas are appropriately marked before their range of action by means of special signs as provided for in the "Provvedimento Generale per la Protezione dei dati personali sulla Videosorveglianza" of the Italian Privacy Authority and in the "Guidelines 3/2019 on processing of personal data through video devices" (hereinafter "Guidelines") of the European Data Protection Board ("EDPB").

The Company, therefore, will process the image of the people who access their premises, displayed and / or recorded through the closed-circuit video surveillance system.



DATA PROCESSING PURPOSES

According to the regulations on the protection of personal data, the processing of personal data carried out by the Company will be based on principles of correctness, lawfulness, transparency and protection of privacy and the rights of individuals.

The video surveillance system was installed with the following purposes:

- a) Ensure the security and safety of airport areas;
- b) Protect the integrity of the company assets and prevent any acts of vandalism or damage;
- c) Organizational and production needs;
- d) Guarantee the safety of the workplace;
- e) Any other purpose prescribed by art. 705 of the Navigation Code, according to which the Airport Manager is entrusted the task, under the control and supervision of ENAC, of coordinating and controlling the activities of the various airport operators present at the airport, and all specific applicable legal provisions.



LEGAL BASIS FOR PROCESSING DATA

The video surveillance activity, for the purposes referred to in the previous points from a) to d), is based on the legitimate interest of the Data Controller (which consists in guaranteeing the security and safety and correct operational organization in the airport areas and in the protection of company assets).

For the purposes referred to in point e), the video surveillance activity is legitimized by legal obligations (in accordance with the provisions of art. 705 of the Navigation Code).



DATA RETENTION PERIOD

The images are kept for 7 days from the moment they were detected. Furthermore, these images may be kept beyond the term indicated therein due to the need to ascertain potentially illegal conduct with respect to the aforementioned purposes, or because of specific requests received by the Police and / or by other Authorities.

The system is programmed in such a way as to operate at the pre-set time the complete automatic cancellation of information, by overwriting, in such a way as to make the deleted data non-reusable.



DATA PROVISION COMPULSORINESS

The refusal to provide data means that the data subject cannot access the Data Controller's premises. Access to video surveillance areas involves the collection, recording, storage and, in general, the use of the images of the data subjects for the purposes previously defined.



PARTIES AUTHORISED TO PROCESS DATA

Data may be processed by employees in company departments who are responsible for carrying out the activities outlined above and have been authorised to process the data and have received suitable operating instructions.



DATA RECIPIENTS

The personal data acquired through the video surveillance system are processed by the companies that carry out supervisory activities on behalf of S.A.C.B.O. S.p.A., appointed as Data Processor under Art. 28 of the GDPR.

The data collected will not be communicated and will not be disclosed to third parties, except in compliance with legal obligations, in particular to Police Forces and other Authorities. These external subjects will process personal data as independent Data Controllers.



DATA TRANSFER OUTSIDE THE EUROPEAN UNION

The collected data will not be transferred outside the European Union.



DATA SUBJECTS' RIGHTS

By contacting the Company via e-mail sent to privacy@sacbo.it data subjects can:

- Ask the Data Controller for access to personal data;
- Object to processing. In any case, the Data Controller reserves the right not to proceed with the request, and therefore to continue processing, in the event that there are compelling legitimate reasons to proceed with the processing that prevail over the interests, rights and freedoms of the data subject;
- Ask the restriction or the deletion of personal data, where applicable.

Data subjects have the right to lodge a complaint to the competent Supervisory Authority.

With regard to the images recorded, the right to correct or amend data as outlined in article 16 GDPR does not apply due to the intrinsic nature of the data (images captured in real time regarding an objective fact). The right to data portability as outlined in article 20 of the GDPR does not apply as the processing is carried out to implement a legitimate interest of the controller.

Data subjects can request to view the images where they have been captured by including a suitable ID document with the request. Responses to access requests cannot include third-party data unless the data can be broken down or have elements removed to render the personal data in question unrecognisable. Such access requests cannot be fulfilled once the aforementioned retention time has elapsed.