European Aviation Safety Agency

PERSONAL DATA PROCESSING RECORDS AND COMPLIANCE CHECK LIST	Ref 056 Video surveillance

Nr.	Item	Explanation
	Facility management Video surveillance	
1.	Last update of this record	01.12.2018
2.	Reference number	056
	Part 1 - Article 31 Record	
3.	Name and contact details of controller	Controller: EASA, Konrad-Adenauer-Ufer 3, 50668 Köln Contact: Head of Corporate Services Department
4.	Name and contact details of DPO	dpo@easa.europa.eu
5.	Name and contact details of joint controller (where applicable)	Not applicable
6.	Name and contact details of processor (where applicable)	Not applicable
7.	Purpose of the processing	The purpose of processing: - Prevention and detection of crime and misconduct - Investigation of criminal offences and misconduct - Investigation of unauthorised, violent or concealed access to the Agency's premises - Investigation of unauthorised access to restricted areas within the Agency - Monitoring of evacuation procedures to ensure safety of staff, visitors and contractors in line with the Agency's physical security policy. In accordance with the applicable law, the Agency might submit video evidence that has been obtained during an investigation, or may have been recorded during normal operation of the system, to substantiate allegations of criminal activity, gross misconduct, or behaviour which puts others as risk. This is only done upon request, normally from the Police, based on their suspecting a criminal act has been committed. The purpose of monitoring staff performance and attendance or presence in the office is excluded from this processing.
8.	Description of categories of persons whose data EASA	The data can include video or images of all persons in the building, e.g. staff, external contractors, consultants, seconded national experts, trainees and visitors.

Nr.	Item	Explanation
	processes and list of data categories	
9.	Time limit for keeping the data	Normally, the data is kept for 7 days, in accordance with the EDPS guidelines. In case of an incident, the time limit can differ, depending on the type of (Police) investigation and/or court proceedings. This is documented in accordance with the EDPS guidelines Annex 5.
10.	Recipients of the data	Recorded video is accessible to the Local Security Health and Safety Officer and the external security Team Leaders only. Live video is also accessible to contracted security guards on duty. In addition, only in case of a criminal offence and upon their request, the data may be made accessible to the Police, upon prior assessment of the request and in accordance with applicable rules and regulations.
11.	Are there any transfers of personal data to third countries or international organisations? If so, to which ones and with which safeguards?	No
12.	General description of security measures, where possible.	The system is operated through a specific IT network, which is protected. A streaming of video footage and a sequence of information from the access control system are available live only in the Security Office and at the Reception after working hours. The PCs of the security team members are password protected and access to the Security Office is restricted to a limited number of staff members. Only specified personnel have authorized access to video-surveillance data. After working hours the system is controlled by the security personnel. Security personnel receives a training to handle confidential information.
13.	For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the privacy statement:	See Privacy statement.