European Aviation Safety Agency

PERSONAL DATA PROCESSING RECORDS AND COMPLIANCE CHECK LIST	Ref 006 Internal Audit

Nr.	Item	Explanation
	Internal Audit	
1.	Last update of this record	01.12.2018
2.	Reference number	006
	Part 1 - Article 31 Record	
3.	Name and contact details of controller	Controller: European Aviation Safety Agency, Konrad-Adenauer-Ufer 3, 50668 Cologne, Germany Contact: Internal Audit and Assurance section Manager, InternalAudit@easa.europa.eu
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 the personal data processing is to facilitate the activities of the Internal Audit Capability (IAC). The IAC is responsible for giving independent and objective opinions on the adequacy and reliability of internal control systems in place, and for making recommendations with the aim to improve the economy, efficiency and effectiveness of the Agency's activities. The IAC assists the ED (Executive Director) and the management of EASA in controlling risks and ensuring compliance with the applicable legislation and rules. In the course of the audit work, the IAC has access to all data held by the Agency and can request access to data held by third parties who have contractual relations with the Agency. As the area of activity of the IAC is very broad, different types of personal data, sometimes even of a sensitive nature, might be processed.
8.	Description of categories of persons whose data EASA processes and list of data categories	Given that this process covers the internal auditing mechanism, data processing mainly concerns EASA staff. External parties could be subject to an audit governed by the Internal Audit mandate.
9.	Time limit for keeping the data	Data is kept for 7 years after the last action resulting from the audit engagement has been assessed as being implemented, in accordance with EASA Records policy.

Nr.	Item	Explanation
10.	Recipients of the data	Auditees and the EASA Directors receive audit and follow up audit reports. If it is a specific action, it is subsequently assigned to someone who was not an original auditee. The IAS request and receive copies of the IAC audit reports each year. Audit files, including test scripts and audit evidence are not shared.
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.	Audit files are stored and maintained electronically on a secure folder on the Agency's shared drive. This folder has restricted access to those staff members of the Internal Audit and Assurance Section.
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.