European Aviation Safety Agency

PERSONAL DATA PROCESSING RECORDS AND COMPLIANCE CHECK LIST	Ref 048 Specific IT technical service

Nr.	Item	Explanation
Specific IT tehnical services		
1.	Last update of this record	01.12.2018
2.	Reference number	048
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: IT Development and Operations Section Manager IT_functional_mailbox@easa.europa.eu
4.	Name and contact details of DPO	dpo@easa.europa.eu
5.	Name and contact details of joint controller (where applicable)	N/A.
6.	Name and contact details of processor (where applicable)	Multiple processors, both internal (IT Administrators) and external (e.g. European Union bodies and suppliers).
7.	Purpose of the processing	The personal data is collected in order to support EASA IT Operations and IT Security.
8.	Description of categories of persons whose data EASA processes and list of data categories	Categories of persons: EASA internal and external users of EASA IT services. Data categories: usernames, emails addresses, EASA Staff photos, cookies, IP related data, access and authorisation related data.
9.	Time limit for keeping the data	• Laptops: lifecycle of the machine (depending on user settings/policies/decision) • N-Drive and network shares: depending on user settings/policies/decision • Email/EV: depending user settings/policies/decision • Work related user data (usernames, emails, photos): as long as needed for the purpose of the process (see point 7), regular clean up exercises performed by IT • Cookies, IP related data, access and authorisation related data: as long as needed for the purpose of the process (see point 7), regular clean up exercises performed by IT

		• Backup: max 12 months
10.	Recipients of the data	• Application Users/Super-users, • Business Service Owners • IT System Administrators to perform operational activities • IT Security officer
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.	Physical access control to IT area (via badge assigned to EASA Staff and Externals cleared by Security). External consultants are requested to provide their criminal records. Non-Disclosure Agreements with external providers Technical IT security measures in place Access to technical services is restricted based on “Need to Know” principle.
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.