European Aviation Safety Agency

PERSONAL DATA PROCESSING RECORDS AND COMPLIANCE CHECK LIST	Ref 051 Communication and collaboration BSO

Nr.	Item	Explanation
	Communication and Collaboration containing: Telephony - Reception Phone System; E-mail : Contact Groups, Functional Mailboxes E-mail - Private Device, Spam Filter	
1.	Last update of this record	01.12.2018
2.	Reference number	051
	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: EASA 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)	N/A.
7.	Purpose of the processing	The purpose of processing personal data is to support EASA IT Operations, Communication 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 Data categories: usernames, emails and email logs, photos, phone numbers, phone logs.
9.	Time limit for keeping the data	• Emails: depending on user settings/policies/decision; • Email logs: as long as needed for the purpose of the process (see point 7); • Work related user data (usernames, emails, photos): as long as needed for the purpose of the process (see point 7); clean up exercises regularly performed by IT. • Backup: Max 12 months
10.	Recipients of the data	• Application Users, • IT System Administrators to perform operational activities

Nr.	Item	Explanation
		• IT Security officer for following up on security incidents and investigations
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 (badge) • External consultants are requested to provide their criminal records, which are kept in accordance with the Access control process. • 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.