



Nr.	Item	Explanation
<b>Clock-in/clock-out system "CICO"</b>		
1.	Last update of this record	1.12.2018
2.	Reference number	031
<b>Part 1 - Article 31 Record</b>		
3.	Name and contact details of controller	Controller: European Aviation Safety Agency, Konrad-Adenauer-Ufer 3, 50668 Cologne, Germany Contact: Head of Human Resources Department; <a href="mailto:hr.info@easa.europa.eu">hr.info@easa.europa.eu</a>
4.	Name and contact details of DPO	<a href="mailto:dpo@easa.europa.eu">dpo@easa.europa.eu</a>
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	<p>The purpose of the personal data processing is the electronic time management system enabling the recording of working time online using a clock-in/clock-out system ("CICO"). The purpose of this system is:</p> <ul style="list-style-type: none"><li>- to facilitate the registration and increase the accuracy of time registration;</li><li>- to ensure the accuracy of time registration. It is necessary to know the actual working time spend on the different activities/projects, in particular when it comes to the invoicing of the services provided by the agency to various applicants (aircraft manufacturers, aircraft maintenance companies, etc);</li><li>- to provide an accurate calculation of flexitime hours.</li></ul> <p>The registration of working time for an EASA staff member is done when the staff member clocks-in to enter the building and clocks-out when leaving the building (staff member's badge is swiped at turnstiles to enter/leave the building or at all entries in the parking area). At EASA premises, the installed card readers are used to register the start time and end time of working hours.</p>



PERSONAL DATA PROCESSING RECORDS AND COMPLIANCE CHECK LIST	Ref 031 CICO Clock-in Clock-out
--	------------------------------------

Nr.	Item	Explanation
		In cases where the use of the installed card readers is not possible, the staff member shall use the manual process to record clock-ins/clock-outs via the IT CATS portal.
8.	Description of categories of persons whose data EASA processes and list of data categories	<p>EASA processes the data of the following data subjects:</p> <ul style="list-style-type: none"> <li>- Temporary agents</li> <li>- Contract Agents</li> <li>- Seconded National Experts (SNEs).</li> </ul> <p>Categories of personal data:</p> <ul style="list-style-type: none"> <li>- First name, surname; personnel number</li> <li>- Concerning leave and absences</li> <li>- Concerning missions and journeys</li> <li>- Other:</li> </ul> <p>Personal information retained for the purposes of Flexitime include: the daily work patterns (time spent in the interests of the service) of the data subject.</p>
9.	Time limit for keeping the data	The collected data are stored in the Relational Database Management System (RDBMS). The retention period for the collected data is 2 years. The period is applicable for the data stored within the CICO terminals. In addition, IT archives the transfer file (CICO data from terminal into SAP) and the same data is stored in SAP.
10.	Recipients of the data	The data subject (i.e. the owner of the CICO data), direct line managers (section manager/Head of Department/Director), time administrator in the HR Department with administrator access rights in SAP, IT staff members with administrator rights in SAP, secretaries/assistants to whom decision has been taken to grant a specific access right to act on behalf on their manager.
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.	Access to CICO and CATS/SAP data is restricted to the subject data holding EASA network credentials as defined in the EASA's "HR" database (i.e. active temporary and contract agents, SNEs). Access to supporting infrastructure is restricted to staff



Nr.	Item	Explanation
		members holding the appropriate authorisations. Only designated staff members can access and change staff members' CICO data (see point 10).
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