



PERSONAL DATA PROCESSING RECORDS AND COMPLIANCE CHECK LIST	Ref 057 Assignment of parking slots
--	--

Nr.	Item	Explanation
Facility management assigning parking spaces and remote controllers		
1.	Last update of this record	01.12.2018
2.	Reference number	057
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 data is processed to enable access and use of the parking facilities and prevent unauthorized access to the parking area.
8.	Description of categories of persons whose data EASA processes and list of data categories	The data collected is from EASA staff members and contains the following data categories: - Name - Function - Car model, colour and registration number - the Staff member also has to fill out and sign a salary deduction form which is kept in EASA Administrative Space Planning (hereinafter: Planon) tool.
9.	Time limit for keeping the data	Collected personal data are uploaded in the Planon tool and stored from the notification of HR Department until access is to be denied, which is usually through notice of cancellation by the user or the end of employment. Documents on owning/returning of the remote control for the parking facilities are kept for 2 years before being destroyed.
10.	Recipients of the data	Process is managed by EASA Corporate Services Department staff members, specifically the Security, Health & Safety Officer. In a framework of the price deduction, the process is managed by the HR Department. The Security Office (external service provider) manages access rights and appropriate use of the facilities.



Nr.	Item	Explanation
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.	<p>Physical security: The server with all the data is located in a locked server room with limited access. A part of the software for the computerised access control system is installed on the computer at EASA's premises. The PC is located in the Security Centre office, to which only a limited number of Staff have access to.</p> <p>Staff security: The security guards are employees of a contracted company. The terms of the contract include confidentiality clauses preventing disclosure of information during the contract period and after the contract terminates.</p> <p>All EASA Staff members receive instructions on confidentiality in processing personal data in accordance with Art. 17 of the staff regulations and through internal training programme.</p>
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.