

## Issuance of Laissez Passer Passport

Nr.	Item	
<b>Header - versioning and reference numbers (recommendation: publicly available)</b>		
1.	Last update of this record	DEC/DIR/2017/010
2.	Reference number:	DPO-043
<b>Part 1 - Article 31 Record (recommendation: publicly available)</b>		
3.	Name and contact details of controller	Controller: EMCDDA, Praça Europa 1, Lisboa, Portugal Contact: Mr. Dante Storti, Head of Administration, EMCDDA security@emcdda.europa.eu
4.	Name and contact details of DPO	Mr. Ignacio Vazquez Molini, DPO, EMCDDA dpo@emcdda.europa.eu
5.	Name and contact details of joint controller (where applicable)	Not applicable
6.	Name and contact details of processor (where applicable)	Mr. Markus Mägerlein, Security Officer, EMCDDA security@emcdda.europa.eu
7.	Purpose of the processing	Issuance of EU travel document for border crossing and within the territory of third countries to EMCDDA staff and relatives.
8.	Description of categories of persons whose data EMCDDA processes and list of data categories	Issuance of the Laissez-Passer (LP) for EMCDDA Staff Members, relatives and associates.  The data categories are limited to the data fields required for a passport. Personal details (name, address etc), Family, lifestyle and social circumstances and Racial or ethnic origin.
9.	Time limit for keeping the data	By the Commission:  -Fingerprints and digital signature are not stored for a longer period than the time necessary to the effective and successful delivery of the EU LP. They are deleted at that time (a few days depending on the day the future holder takes to come and collect the personalised document with a maximum of three months). Nevertheless they remain stored into the chip contained into the laissez-passer under the responsibility of the holder including for their submission to the controls operated at the borders.  -The original application form is kept with the Commission for the corresponding period of validity of the laissez-passer.  - The Commission stores the biographical and the facial image of all the applicants/special applicants, including those belonging to the European Central Bank for a period equivalent to the duration of validity of the EU LP (maximum 6 years) for both for paper and electronic versions.  - The storage includes a period of 3 months maximum of storage extending from the period between the validation of the personalised laissez-passer by the competent staff of the

		<p>Commission service and the moment of its concrete delivery to the future holder, after which the laissez-passer is destroyed if not delivered. This period of 3 months corresponds also to the maximum period of retention for the fingerprints, the precise end of which depends on the day the future holder accepts the personalised laissez-passer and enters in possess (in the meaning of “receives it” as he is not the owner of it).</p> <p>By the EMCDDA:</p> <p>a) For biographical personal data:</p> <ul style="list-style-type: none"> <li>- of the own staff and EU staff members: The retention period follows the general retention period of the personnel file, i.e. 10 years after all rights of the staff member or dependant are extinguished.</li> <li>- of other EU staff members: The data is only stored until the delivery of the laissez-passer booklet to the applicant.</li> <li>- of special applicants, including members of the family, and of ad hoc holders: The retention period should be limited to the duration of validity of the issued EU LP (maximum 6 years) . Personal biographical data, if not kept under other processes are deleted upon expiration of the 6 years validity period running as from the date of issuance of the laissez-passer.</li> </ul> <p>At the end of those retention periods, the biographical personal data are erased.</p> <p>b) For biometrical data there is no retention of biometrical data foreseen hence this data is collected in the enrolement phase. At the expiration of the validity of the EU LP, it must be returned to the Commission to be cancelled and/or partially or totally destroyed. After this process, in case it is cancelled but not totally destroyed, it may be kept by the holder. In this later case, the data (both biographical and biometrical) continue to be accessible on the invalid laissez-passer under the sole responsibility of the holder. Access to biometrics would nevertheless continue to depend on the use of specific technical devices not commercially easily accessible.</p> <p>c) Application form:</p> <p>-A copy of the application form of EMCDDA staff members is stored during the validity period of the laissez-passer. The original form is sent to the central service in Brussels. The data is deleted when the laissez-passer is returned.</p>
10.	Recipients of the data	<ul style="list-style-type: none"> <li>• Requesting staff members</li> <li>• Designated staff members of the EMCDDA’s Staff Info Point,</li> <li>• Designated staff members of the European Commission and the external contractor used by the Commission,</li> <li>• The national authorities responsible for border control including those of third countries,</li> <li>• The authorities in charge of security at the border including airports, maritime or fluvial ports including those of third countries,</li> <li>• The national authority responsible for the management of lost and/or stolen document including those of third countries,</li> <li>• The Court of justice and the national jurisdictions within the remit of their competences including those of third countries,</li> <li>• The disciplinary bodies in the institutions, notably IDOC,</li> <li>• OLAF,</li> <li>• The Auditors,</li> <li>• Europol,</li> <li>• Interpol, SIS II, Sirene.</li> <li>• CEPOL,</li> </ul>

		<ul style="list-style-type: none"> <li>The central alert system 24/7 within the remit of its competences and on a need-to-know basis.</li> </ul>
11.	Are there any transfers of personal data to third countries or international organisations? If so, to which ones and with which safeguards?	<p>Yes</p> <ul style="list-style-type: none"> <li>The national authorities responsible for border control including those of third countries,</li> <li>The authorities in charge of security at the border including airports, maritime or fluvial ports including those of third countries,</li> <li>The national authority responsible for the management of lost and/or stolen document including those of third countries,</li> <li>The Court of justice and the national jurisdictions within the remit of their competences including those of third countries,</li> <li>Interpol, SIS II, Sirene.</li> </ul>
12.	General description of security measures, where possible.	<p>The EU Laissez-Passer pre-enrolment centre in Lisbon will be equipped with one pre-enrolment workstation, storing the data captured during pre-enrolment on a secured drive.</p> <p>The data captured during pre-enrolment must be transmitted to Brussels for preparation of the file sent to the contractor manufacturing the Laissez-Passers. To this end, an end-to-end transmission between the local data transmissions workstations of Lisbon and Brussels must take place.</p> <p>The local data transmission workstation, must be located in a secure room with access control system.</p> <p>The file transfer from data transmission workstation in one location to that in another location is done via a dedicated encrypted functional e-mail with certificates.</p>
13.	For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the privacy statement:	<p><a href="http://ec.europa.eu/dpo-register/details.htm?id=38550">http://ec.europa.eu/dpo-register/details.htm?id=38550</a>.</p>