EUROPEAN DATA PROTECTION SUPERVISOR

WOJCIECH RAFAŁ WIEWIÓROWSKI
ASSISTANT SUPERVISOR

[…]
Head of Air Crew & Medical Department
European Aviation Safety Agency
Postfach 10 12 53
Cologne
Germany

Brussels, 19 July 2016
WW/OL/mv/ D(2016) 1554 **C 2016-0271**
Please use edps@edps.europa.eu for all correspondence

Subject: EASA notification for prior checking "European Aero-Medical Repository" (EAMR) project

Dear […],

On 10 March 2016, EASA's acting Data Protection Officer […] notified the European Aero-Medical Repository (EAMR) project to the EDPS for prior-checking under Article 27 of Regulation (EC) 45/2001[1] ("the Regulation").

On 22 March and 30 April 2016, the EDPS asked several questions for clarification, suspending the case; answers were received on 20 April and 3 May 2016. On 2 June 2016, the EDPS shared the draft analysis with EASA to confirm that it correctly reflected the facts of the case; EASA requested a meeting, which took place on 22 June 2016 and provided comments on 11 July 2016; the case was suspended in the meantime.

Please find below a summary of the facts of the case at hand, as well as the EDPS' legal analysis and recommendations.

The Facts

The EAMR will[2] be a repository of information related to the class 1 medical certification[3] of pilots. Such pilots can apply for medical certification in any EASA Member State.[4] The

[1] OJ L 8, 12.1.2001, p. 1–22
[2] The project is currently in development; the start of operations is planned for December 2016.
[3] See Commission Regulation (EU) No 1178/2011, OJ L 311/1, 25/11/2011, Annex IV, MED.A.030. Class 1 medical certification is required for applicants for and holders of a commercial pilot licence (CPL), a multi-crew pilot licence (MPL), or an airline transport pilot licence (ATPL).
[4] EU-28 plus Norway, Iceland, Switzerland and Liechtenstein

business case for EAMR is to avoid non-declaration of medical issues and forum shopping by pilots by facilitating information sharing between National Aviation Authorities (NAA), aero-medical examiners (AME)[5] and aero-medical centres (AeMCs)[6] in order to ensure a high level of safety in commercial aviation.[7]

As part of their examinations to determine whether they are fit to fly and should receive a class 1 medical certificate, pilots/applicants for a pilot licence have to provide a declaration on earlier examinations, denials, suspensions and revocations of medical certificates. EAMR will allow NAAs/AMEs to more easily cross-check these self-declarations[8] by automatically informing them if an applicant already has an entry in the system and whether the information is consistent. If not, e.g. if a pilot declares never having had a certificate suspended, while EAMR contains information on a past suspension, the system will alert the AME, identifying the record and the competent authority to be contacted to clarify the situation.[9] Information on medical certificates issued (see below) will be fed into EAMR by the NAAs for administrative data (this may be delegated for AME, AeMCs and medical assessors) and by AMEs, AeMCs and Medical Assessors for information on the certificates issued by them.

EAMR will be a repository for these certificates, but will also perform some automated cross-checking.[10] EASA will not itself take decisions on granting/denying/suspending/revoking certificates, but will act as a service provider for EAMR, providing it for NAAs / AeMCs / AMEs to use. It will host EAMR and ensure operational management. Except for maintenance and administration, EASA will not have access to the content of the system, except for using de-identified information for standardisation purposes.

EASA intends to base EAMR on Articles 15(1) and 38(3)(e) of Regulation (EC) No 216/2008; Commission Regulation (EU) 1178/2011 further details the rules, notably in the following parts of the annexes:

- ARA.GEN.200 (c) - NAAs shall have procedures for mutual exchange of information;
- ARA.GEN.220(a)(5) - record-keeping requirements for certificates;
- ARA.MED.130 - format of medical certificate;
- ARA.MED.150 (a) - NAAs to keep information on medical examinations;
- ARA.MED.150 (b) and ARA.MED.150 (c) - 10 years retention for medical records of licence holders;
- MED.A.035(b)(2)(ii) and MED.A.035(b)(2)(iii) - format of application and declaration on earlier examinations;
- ARA.GEN.220(a)(5) - default 5 years retention for other data.

EAMR will not contain the entire medical file, but only a limited amount of information – identification and contact data for the pilot, licensing authority, date of examination, date of issue of certificate and expiry date, whether a certificate has been denied / has been or is suspended / has been or is revoked or whether limitations have been/are currently imposed (all

[5] AME are specialised medical professionals accredited for issuing medical certificates for pilots.
[6] AeMC are medical facilities specialised in aviation medicine; their staff includes AMEs.
[7] EAMR is also meant to streamline procedures for revalidation or renewal applications in a different Member State than the one in which the initial certificate was issued.
[8] In the current system, a NAA can ask *all* other NAAs if they hold relevant information about an applicant/pilot. However, this requires a significant effort from both requesting and answering NAAs and according to EASA is not practically feasible in a systematic way.
[9] See p. 13Wp15/FS3-01,18/12/2015
[10] E.g. alerting NAAs to certificate records that have been left pending for a long time, possible duplicate applicant records, alerting users to inconsistencies between declarations of pilots/applicants and information already included in EAMR, etc.

yes/no), the medical professional who issued the certificate and the relevant competent authority for the assessor. This will relate both to current and to past certificates.

The actual test results, photos of pilots and reasons for denials / suspensions / revocations will not be included in the EAMR.

EAMR will process personal data of two different categories of persons (data subjects):

1. pilots/applicants for medical certificates: their data will be stored as explained above;
2. AMEs & medical assessors: their contact information (constituting personal data) will be included in certificates issued;

EASA will develop a data protection notice and will instruct licensing authorities to make it available to data subjects, either by individual notification or by publication.

Whenever a record is created or updated, an e-mail notification will be sent to the pilot/applicant, containing a read-only access code allowing her/him to check the information directly in EAMR, providing a means for them to obtain access to personal data held about them. Apart from this, EASA does not intend to provide access to their own data for pilots/applicants. Requests for rectification are to be sent to the competent licensing authorities in the Member States (outside EAMR).

AME and AeMCs may also be based in countries outside the EU/EEA. EASA does not expect that more than 1% of the transactions in the system will be made from outside the EU/EEA.[11]

Data from the certificates will be kept for 10 years after the expiration of the latest medical certificate; other data (e.g. account information of AMEs) will be kept for 5 years.

[…]

EASA notified EAMR for prior checking mentioning Articles 27(2)(a) (data relating to health) and (b) (processing operations intended to evaluate).

Legal Analysis

Need for prior-checking

Article 27 of the Regulation subjects a number of "risky" processing operations to prior checking by the EDPS. The criteria are listed in paragraph 2 of that Article and include among others the processing of health data (point (a)) and processing operations intended to evaluate personal aspects of the data subject (point (b)). Such processing when carried out by an EU institution or body as controller[12] is subject to prior checking. It should be noted that there may be situations of "joint controllership", where several entities together are responsible.

EAMR will be operated by EASA, but based on the information provided will basically act as a repository for information provided to it. The situation is one of joint controllership: EASA fulfils some tasks of a controller (determining the technical means of the processing, ensuring security…), while the other parties involved fulfil other tasks of a controller (entering data, ensuring data quality…). They are thus joint controllers.

[11] Individual AMEs established in countries outside the EU/EEA are attached to a "home" NAA in the EU/EEA. For AeMCs in third countries, EASA is the competent authority similar to the NAAs for AeMCs established in the Union (Regulation (EU) 1178/2011 ARA.MED.A.001). However, the individual AMEs working in such AeMCs are subject to the rules of their "home" NAA. EASA's role only extends to organisational aspects of the work of the AeMC, which are not relevant for EAMR. Additionally, currently no such AeMCs outside the EU/EEA exist.

[12] See Article 2(d) of the Regulation.

Against this background, it has to be noted that EASA *itself* does not carry out an "evaluation" of pilots/applicants in the sense of Article 27(2)(b) of the Regulation. EAMR is a repository for the decisions taken at the national level.[13] A similar reasoning applies to the processing of health data in EAMR: EASA will only act as a *repository* of information provided.[14]

Therefore, EAMR does not trigger Article 27 of the Regulation. It should be noted that the medical examinations and assessments are carried out on the national level and under the supervision of the competent national data protection authority, while EASA's role in EAMR is basically that of a repository. That being said, the EDPS still has several recommendations to make in order to ensure that EAMR will comply with the Regulation. The analysis below does not cover all aspects of the Regulation, but only those which require improvements or otherwise give rise to comments.

Legal basis

The legal bases quoted by EASA relate to the exchange of information between competent authorities. The main change brought about by EAMR compared to the current situation is that there will be a centralised system hosted by EASA.

EASA sees Article 5(a), i.e. necessity for the performance of a task attributed to it in the public interest, as the ground for lawfulness. Additionally, Article 10 has to be considered, as part of the information in EAMR will relate to health.

The legal provisions quoted by EASA in the documentation provide a solid legal basis for information exchanges between the different parties; Article 15(1) of Regulation 216/2008 states that "the Agency and the national aviation authorities shall exchange any information available to them in the context of the application of this Regulation and its implementing rules"; the annexes to Commission Regulation 1178/2011 then further spell out these exchange requirements.

However, these legal bases only lay down an obligation for the different stakeholders involved to cooperate and exchange information (including on current and past certificates when necessary for the medical examination); they do not establish a central repository of current and past certificates to be provided by EASA.[15]

Article 10 of the Regulation contains specific rules on the processing of special categories of data, including data relating to health. Paragraphs 2 to 4 of Article 10 list the conditions under which data relating to health may be processed. None of the points in Article 10(2) apply.[16] Neither does Article 10(3), as EAMR in itself is not a medical diagnostic tool or otherwise

[13] This is the same logic as the one explaining why, although they contain sensitive data and information about evaluation, the management of the personal files to be kept under the Staff Regulations is not subject to prior checking: the personal file is only a repository for the outcome of other processing operations, who themselves may be subject to prior checking (e.g. staff appraisal). See e.g. EDPS case 2013-1365, available at https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Priorchecks/Opinions/2014/14-03-18_personal_files_INEA_EN.pdf

[14] See EDPS case 2015-0138, non-prior check opinion available at: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Priorchecks/Opinions/2015/2015-06-03_Goalkeeper_software_environment_EEAS_EN.pdf.

[15] See also EDPS case 2013-1296, available at: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Priorchecks/Opinions/2016/16-05-18_OLAF_PC_EN.pdf.

[16] Point (a) [express consent] does not apply as there is no possibility to refuse to be included in EAMR; point (b) [rights and obligations of the controller under employment law] does not apply as EASA (as controller) is not the employer of applicants/pilots; points (c) to (e) obviously do not apply either.

linked to providing medical care.[17] Finally, Article 10(4) of the Regulation provides that the general prohibition of processing special categories of data can be lifted if, "subject to the provision of appropriate safeguards, and for reasons of substantial public reasons of substantial public interest" an exemption is "laid down in the Treaties […] or other legal instruments adopted on the basis thereof".

Given the amount of sensitive data that will be processed in EAMR, **a solid legal basis for *establishing a central repository* is needed for EAMR to be lawful under Article 5(a) and also in order to comply with Article 10(4).**

Such a legal basis could for example be created via an amendment to Commission Regulation (EU) 1178/2011 or other decision at the appropriate level. The EDPS also takes note that Article 63(2) to (8) of the Commission proposal[18] for replacing EASA's founding regulation contains provisions that - if adopted as proposed - could provide a legal basis in the future; paragraph 8 of that Article contains an authorisation for the Commission to lay down detailed requirements in implementing acts, including data protection requirements. In any case, a legal basis needs to be present before the system can start processing personal data in production usage.[19]

Transfers outside the EU/EEA

Some AMEs/AeMCs may be established in countries outside the EU/EEA. This means that some use of the system will result in transfers of personal data outside the EU/EEA, which is subject to specific rules both in national data protection legislation[20] and in Regulation 45/2001. As far as Regulation 45/2001 is concerned, the EDPS has outlined its approach to such transfers in a position paper.[21]

The EDPS understands that AMEs established outside the EU/EEA using EAMR will be attached to a NAA in the EU. These NAAs are also responsible for managing their user populations, including AMEs established outside the EU/EEA. Compliance with the rules on transfers of personal data outside the EU/EEA would then be that NAA's responsibility.

The fact that AMEs/AeMCs established outside the EU/EEA fulfil their roles according to the rules of Commission Regulation 1178/2011 may not as such be sufficient to ensure compliance with the transfer rules in national legislation. EASA should draw NAAs' attention to this point.

Data subjects' rights: information and access

EASA does not collect the information to be included in the EAMR directly from the data subjects (notably pilots/applicants). As concerns the right of information, EASA is therefore in the situation of Article 12 of the Regulation and has the obligation to inform data subjects about the processing unless this proves to be "impossible or would require a disproportionate effort" (Article 12(2) of the Regulation). This has to be done "at the time of undertaking the recording of personal data or, if a disclosure to a third party is envisaged, no later than the time when the

[17] EAMR is a tool for AMEs to double-check the declarations made by pilots/applicants; its purpose is to detect non-declaration, not to provide diagnosis/treatment/care for detected issues.
[18] COM(2015)0613, 07.12.2015
[19] […]
[20] Currently, the provisions implementing Articles 25 and 26 of Directive 95/46/EC (OJ L 281, 23.11.1995, p. 31–50); as of 25 May 20918, Chapter V of Regulation (EU) 679/2016 (OJ L 119, 4.5.2016, p. 1–88).
[21] Position paper on the transfer of personal data to third countries and international organisations by EU institutions and bodies, available at: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Papers/14-07-14_transfer_third_countries_EN.pdf, see notably p. 9 on "pull" access.

data are first disclosed" (Article 12(1) of the Regulation). The usual way of providing this information are short data protection notices made available to data subjects.

In the case at hand, EASA will have the e-mail addresses of data subjects. Sending an automatic e-mail with the data protection notice or a link to it does not appear to require a disproportionate effort. **EASA should therefore inform data subjects accordingly**.[22] Concerning pilots/applicants, this information can be included in the message informing them about the creation of an entry. Concerning AMEs/assessors, information should be made available to them when their accounts are created.

The right of access to one's own personal data under Article 13 of the Regulation notably gives data subjects the right to obtain a copy of the personal data processed about them by a controller. EASA plans to have this right exercised via the NAAs and does not plan to provide access itself. As concerns entries in the EAMR, EASA will provide a message to pilots/applicants with an access code allowing them to access their records in EAMR. This already provides access to their own data processed in EAMR for pilots/applicants.

Thus, EASA in fact already plans to provide access in the case of creation or updates of records; there also appears to be no reason why a restriction under Article 20 of the Regulation would be necessary, and no such need has been invoked by EASA either. Therefore, EASA **should also provide access in reply to other queries from data subjects**.

Security
[…]

Conclusion

Although the processing operations notified are not subject to prior checking under Article 27 of the notification, the EDPS has made several recommendations to ensure compliance with the Regulation. To recapitulate, these are:

- establish a solid legal basis for *a central repository* of information related to medical certificates;
- inform data subjects about the processing of their personal data;
- provide access to their own personal data in reply to other queries from data subjects;
- […]

Please report back on the implementation of these recommendations within 3 months of the date of this Opinion.

Yours sincerely,

[signed]

Wojciech Rafał WIEWIÓROWSKI

[22] NAAs are required under national legislation to provide information on *their* processing of personal data, including information on the recipients of the personal data *they* collect, which will then include EASA.

CC: […], DPO, EASA
[…], Legal Adviser/acting DPO, EASA
[…], Deputy Head of Aircrew and Medical Department, EASA