EUROPEAN DATA PROTECTION SUPERVISOR

WOJCIECH RAFAŁ WIEWIÓROWSKI
ASSISTANT SUPERVISOR

[…]
Head of Rights and Obligations Division – BA.HR.3
European External Action Service

Brussels, 14 December 2017
WW/OL/sn/D(2017)2756 **C 2016-0780**
your ref.: e-dpo 1585
Please use edps@edps.europa.eu for all correspondence

**Subject: Prior-checking Opinion regarding the activities of the EEAS' medical service (EDPS case 2016-0780)**

Dear […],

On 1 September 2016, the European Data Protection Supervisor (EDPS) received a notification for prior checking under Article 27 of Regulation (EC) No 45/2001[1] ("the Regulation") on the activities of the medical service of the EEAS from the Data Protection Officer (DPO) of the EEAS (EEAS reference e-dpo1585)[2].

The EDPS has issued Guidelines concerning the processing of health data[3] ("the Guidelines"). Therefore, this Opinion analyses and highlights only those practices that do not seem to be in conformity with the principles of the Regulation and with the Guidelines. In the light of the accountability principle guiding his work, the EDPS would nonetheless like to highlight that *all* relevant recommendations made in the Guidelines apply to the processing operations put in place for the processing of health data at the EEAS.

## 1. Facts

The notification mentions a number of services provided by the EEAS' medical service:

1. Health-related advice/support by phone, by mail or in person. This includes individual medical and psychological advice/support and health advice related to reintegration after sickness leave. Data subjects for this part may be staff members in delegations and their family members covered under the Joint Sickness Insurance Scheme (JSIS).
2. The EEAS medical service also provides pre-posting medical advice and training upon request. The EEAS confirmed that this related to providing information such as

[1] OJ L 8, 12.1.2001, p. 1.
[2] As this is an ex-post case, the deadline of two months does not apply. It has been suspended for further information from the EEAS from 6 September to 20 October 2016, from 8 to 23 December [unsuspended first following EDPS working day, i.e. 3 January 2017] and for comments on the draft Opinion from 24 November to 11 December 2017. This case has been dealt with on a best-effort basis.
[3] Available on the EDPS website: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Guidelines/09-09-28_Guidelines_Healthdata_atwork_EN.pdf

recommended vaccinations and good health practices for staff before taking up a post abroad.

3. Advice for to the administration related to fitness to work, invalidities, early rotation for medical reasons (EEAS staff Brussels, European Commission and EEAS staff in EU Delegations, Local Agents in Delegations).
4. Advice to the administration related to the evaluation of the Living Conditions Allowances (advice regarding the Health Parameter). EEAS later confirmed that this was general advice on conditions in third countries, so no personal data related to health would be processed here.
5. The Medical Service could also provide an on-the-spot support and medical help in case of crises or to visit hospitals abroad to assess the quality of medical care (for the latter: general assessment, no processing of personal data related to health).
6. For annual screenings, pre-recruitment exams and fitness to work evaluations, the EEAS relies on the European Commission's medical service, which carries out these tasks for the EEAS under a service level agreement.

The EEAS has submitted a separate notification for medical evacuations.[4]

The EEAS will only share medical information strictly speaking with other medical services and the JSIS medical advisor. Confidential medical information will not be shared with non-medical recipients, except with the consent of the data subject. Related documents (e.g. for appeals procedures) may be shared more widely, as needed. The privacy statement lists a number of recipients for these purposes.

Concerning individuals' right to access their own data, the notification referred to possible restrictions under Article 20(1)(a) of the Regulation. The EEAS later clarified that the same rules as for the EC's medical service apply.

The retention period for medical data is 30 years after leaving the service, as per the European Commission's Common Retention List.

## 2. Legal analysis

### 2.1. Information about recipients of personal data

The Regulation contains specific rules on transfers of personal data, within/between EU institutions (Article 7 - e.g. to the appeals unit in case of an appeal), to recipients subject to legislation implementing Directive 95/46/EC (Article 8 - e.g. a hospital or a medical practitioner in au EU Member State) and to other recipients (Article 9 - e.g. a medical practitioner in a third country). People have to be informed about the (categories) of recipients of their personal data (Article 11(1)(c)).

The privacy statement for the activities of the medical service contains a long list of possible recipients. As currently drafted, the list is not very clear.

The privacy statement also refers to the person concerned (data subject) as a recipient of personal data. Please note that making their own personal data available to data subjects themselves does not fall under the transfer rules.

The EDPS **recommends** improving the privacy statement by organising the list of recipients in a clearer way. People affected should be able to understand easily who may receive which data in which circumstances.

[4] EEAS reference e-dpo 1586 / EDPS reference 2016-0778.

### 2.2. Right of access

According to Article 13 of the Regulation, persons have the right of access to the personal data EU institutions process about them. Some restrictions are possible under Article 20 of the Regulation.

In the notification, the EEAS referred to possible restrictions under Article 20(1)(a) of the Regulation. This point relates to restrictions that are necessary to safeguard "the prevention, investigation, detection and prosecution of criminal offences".

This exception does not appear to be relevant here. There is no obvious situation in which denying persons access to *their own* medical data would appear to be necessary for the protection of such investigations.

The only exception in Article 20 that may possibly be relevant here is Article 20(1)(c), "the protection of the data subject or of the rights and freedoms of others". This could e.g. be relevant for data of a psychological or psychiatric nature. For such data, access can be provided indirectly via a medical professional, if an assessment made on a case-by-case basis reveals that indirect access is necessary for the protection of the data subject, given the circumstances. As a rule, the EEAS has to grant people access to their own health data.

The EDPS **recommends** that the EEAS grant persons access to their own data to the widest extent possible. In the rare cases in which restrictions of access may be justified under Article 20 of the Regulation, the EEAS should document its reasons for restricting access.

### 2.3. Retention periods

The EEAS states that it keeps medical data in line with the European Commission's Common Retention List. This period appears to apply to the medical file as such, which according to the information provided, is kept by the EC medical service as a processor, not the EEAS medical service itself. This appears to cover the activities mentioned under point 6 in the description of the facts above (annual screening, pre-recruitment exams etc.). The EEAS did not provide information on the applicable retention period for the other activities it carries out itself (points 1 to 3 and the first part of point 5 in the description of the facts). It appears that many of these activities may not require such long retention periods. It is for the EEAS to assess its storage needs here and to define appropriate retention periods.

The EDPS **recommends** that the EEAS define and enforce retention periods in line with its needs for the activities it carries out itself. The EEAS should document its reasons for the retention periods chosen.

### 2.4. Relationship with EC medical service

The European Commission's medical service carries out the annual screenings, pre-recruitment exams and fitness to work evaluations for EEAS staff under a service level agreement (SLA)[5].

Practically speaking, the EC medical service seems to act as a processor for the EEAS here. This means that the EC medical service shall only act upon EEAS instruction here and that the EEAS remains accountable for the whole of the processing.

[5] Under the SLA the EEAS Medical Service has access for consultation to the medical files of EEAS staff and EC staff in EU Delegations in the EC medical database, SERMED. The medical cell has medical data of EEAS and EC personnel in Delegations.

The SLA mainly covers financial aspects of the different services provided. It does not specifically state that the EC medical service shall act only upon instruction from the EEAS (as controller). Such instructions can also take the form of general standing instructions.

Looking forward, the new data protection regulation for EU institutions, bodies and agencies[6] will most likely provide for more detailed rules in controller-processor and controller-controller relationships[7]. The EEAS would do well to review the SLA in the light of upcoming obligations.

The EDPS **recommends** ensuring that the SLA with EC medical service will conform to the new requirements by the time the new data protection regulation for EU institutions will become applicable.

### 2.5. Other points

In point 11 of the notification form, the EEAS refers to the Financial Regulation, citing Council Regulation (EC, Euratom) No 1605/2002[8]. This text has since been replaced by Regulation (EU, Euratom) No 966/2012[9] with functionally equivalent content.

## 3. Conclusion

In this Opinion, the EDPS has made several recommendations to ensure compliance with the Regulation, as well as several suggestions for improvement. Provided that both major and minor recommendations are implemented, the EDPS sees no reason to believe that there is a breach of the Regulation.

The EDPS expects **implementation** for the recommendations made in this Opinion:

1. Improving the privacy statement by organising the list of recipients in a clearer way. People affected should be able to understand easily who may receive which data in which circumstances;
2. Granting persons access to their own data to the widest extent possible. In the rare cases in which restrictions of access may be justified under Article 20 of the Regulation, the EEAS should document its reasons for restricting access;
3. Defining and enforcing retention periods in line with its needs for the activities it carries out itself. The EEAS should document its reasons for the retention periods chosen;
4. Ensuring that the SLA with EC medical service will conform to the new requirements by the time the new data protection regulation for EU institutions will become applicable.

In light of the accountability principle, the EDPS expects that the EEAS implement the above recommendations accordingly and has therefore decided to **close the case**.

Yours sincerely,

[signed]

Wojciech Rafał WIEWIÓROWSKI

[6] Proposal COM(2017)8 final, still in the legislative process, planned applicability 25 May 2018. See especially Article 29 of that proposal.
[7] See also EDPS letter of 12 October 2017 (our reference D(2017)2101 in case 2016-1153).
[8] OJ L 248, 16.9.2002, p. 1.
[9] OJ L 298, 25.10.2012, p. 1, as amended.

Cc: […], DPO, EEAS
[…]