EUROPEAN DATA PROTECTION SUPERVISOR

WOJCIECH RAFAŁ WIEWIÓROWSKI
ASSISTANT SUPERVISOR

[...]
Head of Division
EEAS.BA.HR.5 Local Agents
European External Action Service (EEAS)
9A R.P. Schuman
Brussels 1046
Belgium

Brussels,
WW/SS/sn/D(2018)1510 **C 2017-0986**
Please use edps@edps.europa.eu for all correspondence

Subject: **Prior-checking Opinion regarding the reimbursement of medical expenses under the Complimentary Sickness Insurance Scheme for Local Agents in EU Delegations (EDPS case 2017-0986)**

Dear [...],

On 14 November 2017, 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 reimbursement of medical expenses under the Complimentary Sickness Insurance Scheme for Local Agents in EU Delegations (CSISLA) from the Data Protection Officer (DPO) of the EEAS.[2] The EEAS and EU Delegation to each specific third country and international organisation are co-controllers for this processing operation.

The EDPS has issued Guidelines concerning the processing of health data in the workplace by Union institutions and bodies[3] (the Guidelines). Therefore, this Opinion analyses and highlights only those practices, which 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 of local agents by the EU Delegations and EEAS.

The EDPS has already previously stated that the data collected in connection with the management of a sickness insurance scheme constitutes health data[4]. The processing of data

[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. The case was suspended from 21 November 2017 to 6 March 2018 and from 12 to 28 June 2018. This case has been dealt with on a best-effort basis.
[3] Available on the EDPS website: https://edps.europa.eu/sites/edp/files/publication/09-09-28_guidelines_healthdata_atwork_en.pdf

[4] See e.g. EDPS Opinion of 10 July 2007 in case 2004-0238, available on the EDPS website: https://edps.europa.eu/sites/edp/files/publication/07-07-10_commission_sickness_insurance_en.pdf.

related to health is likely to present specific risks to the rights and freedoms of data subjects in accordance with Article 27(2)(a) of the Regulation.

In order for a reimbursement request for a medical expense to be considered justified, the local agent must provide in the reimbursement form information on the type and nature of the exam, medicine etc. with the supporting documents (original invoices and medical prescriptions, medical report).

The data, including personal data, processed are the following:
- name forename, address, date of birth, personal ID number of the local agent;
- name forename, address, date of birth, relation with local agent of the eligible dependant;
- data in reimbursement form relating to the type of performer of services and the nature of expenses claimed;
- supporting documents (medical practitioner's prescription, invoice) and medical report (treatment, foreseen treatment, plaster model, complete diagnosis, health conditions, X-rays, medical practitioner's prescription), in particular, in case of prior authorisation requests;
- credentials of the practitioners.

The Guidelines recommend[5] that, in line with Articles 4, 5(a) and 10(3) of the Regulation, the claims for reimbursement of medical expenses should only be processed by the specific department responsible for handling these claims, who validates them and only transmits to the budget and payment department the total sum to be reimbursed. In accordance with the principle of necessity as laid down in Article 7, no medical or health information (e.g. data indicating the type of exam or treatment carried out or the speciality of the medical practitioner) should be communicated to the budget and payment department. Furthermore, in no circumstances should any data contained in these claims be communicated to the Human resources department.

The procedure implemented by the EEAS and EU Delegations for the reimbursement of medical expenses under the CSISLA differs from what the EDPS recommends in the Guidelines. The EEAS explained that the EEAS does not have a medical service for local agents and the reimbursement of medical costs is decentralised to Delegations and that therefore, the procedure recommended by the EDPS in the Guidelines cannot be applied to the reimbursement of Local Agents' medical costs.

Reimbursement requests must be submitted and dealt with at Delegation level and not sent to the EEAS Headquarters (EEAS BA.HR.5 Division). The request for reimbursement (request form and supporting documents) is lodged by the local agent in a sealed envelope addressed to the Head of Administration and marked 'Medical Matter'. The initiating agent then draws up a summary of the proposed reimbursement, including the main items of information needed for processing the reimbursement: names of local staff member and beneficiary, type of expense and amount of the reimbursement proposed. The Head of Administration verifies the file (including support documents) and re-seals the envelope containing the supporting documents. The Head of Delegation authorises the payment on the basis of the summary and of the reimbursement request form; the supporting documents, placed in a sealed envelope, may be checked if this is deemed necessary.

The EEAS explained that the number of people required to handle the reimbursement of local agents' medical costs is reduced to the strict minimum. Only three persons have access to the request form (also called claim form): the initiating agent, the Head of Administration (verifying agent) and the Head of Delegation (authorising officer). The members of the Delegation staff whose duties are likely to bring them into contact with data of a medical nature must sign a specific confidentiality declaration. This declaration contains the staff member's undertaking not to reveal such medical data or his/her interpretation thereof and not to use it in

[5] See specifically pages 6, 7 and 13 of the Guidelines.

an unauthorised manner, as well as an acknowledgement that she/he will be liable to penalties if she/he does not fulfil the obligation to maintain confidentiality.

The EDPS takes note of the above measures taken by the EEAS and EU delegations (limited number of people handling the reimbursement requests, signature of specific confidentiality declarations) to comply with the Regulation, in particular with Articles 5(a) and 10(3) thereof.

Nevertheless, the EDPS considers that the **procedures and tools** in place at the EU Delegations and the EEAS Headquarters for the reimbursement of medical expenses under the CSISLA **should be improved** in view of the risks to the rights and freedoms of individuals whose personal data are processed.

In particular, the risks of unfairness of processing, discrimination, further use for different proposes of the data collected, unauthorised disclosure of data and other security risks may be higher when sensitive data is processed in a small environment like an EU Delegation by staff who are not medical professionals or health insurance specialists. The EDPS therefore **recommends** that the EEAS and EU Delegations **re-evaluate those procedures and tools to mitigate those risks**. For example, the EEAS and EU Delegations could centralise the reimbursement of medical expenses under the CSISLA to minimise the possible negative effects of colleagues in the same Delegation having this sensitive information.

The new legal framework will bring increased accountability of the EU institutions and bodies in how they process personal data and stricter obligations for compliance with data protection rules. In line with the accountability principle, the EEAS and EU Delegations have to ensure compliance and be able to demonstrate it where requested.

In preparation for the new legal framework, the EDPS **recommends** that the EEAS and EU Delegations **conduct a threshold assessment** on the processing of personal data under the CSISLA to verify whether it will require a data protection impact assessment (DPIA) under Article 39 of the upcoming rules.[6] If the need for a DPIA is confirmed, the EEAS and EU Delegations should start the **DPIA** process immediately.

In light of the accountability principle, the EDPS expects the EEAS and EU Delegations to implement the above recommendations accordingly.

The EEAS has informed us that it is in the process of merging the notifications and streamlining the procedure anticipating the EDPS' recommendations and the upcoming data protection rules. The Regional Centre for Europe (a department set up within the EEAS) has been established to function as a central service. It handles and administers reimbursements for 27 Delegations, with less risk of further disclosure of personal data. The EEAS is also assessing the security measures to safeguard the integrity and confidentiality of the medical data. According to EEAS, the idea is to further expand this activity for other delegations.

We thank you for your continued cooperation in enhancing compliance with data protection rules. The EDPS has therefore decided to **close the case 2017-0986**.

Yours sincerely,

[signed]

Wojciech Rafał WIEWIÓROWSKI

Cc.: [...], DPO, EEAS

[6] See legislative procedure 2017/0002(COD).