Opinion on a notification for Prior Checking received from the Data Protection Officer of the European Centre for Disease Prevention and Control regarding the provision of confidential staff counselling

Brussels, 22 April 2016
(Case 2013-0790)

1. Proceedings

On 1 July 2013, the European Data Protection Supervisor (EDPS) received a notification for prior checking under Article 27(2) of Regulation (EC) No. 45/2001 (the Regulation) relating to the processing of personal data in the context of providing confidential staff counselling from the Data Protection Officer (DPO) of the European Centre for Disease Prevention and Control (ECDC).

Given that this is an ex-post case, the deadline of two months for the EDPS to issue his Opinion does not apply. Additional information regarding the notification was sent by ECDC on 3 July 2013. Further information regarding the notification was requested from ECDC on 19 August 2014, to which ECDC replied on 29 August 2014. The draft Opinion was sent to the DPO for comments on 19 January 2015. The EDPS received a reply on 27 January 2015.

2. Details of the processing operation

The counselling service for ECDC staff is provided by an external psychological and psychotherapeutic clinic, on a contractual basis. The short-term confidential counselling is available to statutory staff and seconded national experts. ECDC staff may address different issues to the counsellor, possibly also alleged harassment. Each staff member is entitled to five counselling sessions per calendar year. No reporting on individual issues may be requested by ECDC from the clinic.

Appointments are confidential and are booked by the staff member through the ECDC in-house doctor. The recommendation for counselling support can also come from the ECDC Human Resources (HR), should a staff member turn to the ECDC HR for assistance in this matter. Although the referral will be made by the organization, the content of counselling exchange between the counsellor and the employee will be strictly confidential.

Employees are issued tickets which will allow them to access counselling services within a specific period of time. According to the notification, the ticketing system serves primarily the purpose of anonymity of the users of the counselling services and also to provide evidence for due diligent budget expenditure. No information about the ECDC staff members requesting counselling support will be recorded and kept by ECDC. A register which identifies a certain ticket number with a staff member is kept only by the clinic, while the ECDC keeps track of the ticket numbers only.

While the clinic retains data for 10 years from the last input in the counselling journal, the ECDC has not considered defining a retention period for the ticket numbers, which are electronically stored.

For confidentiality reasons, there is no intention from ECDC to link the two registers – one of the 'counselling ticket numbers' kept by ECDC for budgetary purposes and the second related to the names of staff using the counselling services that are kept by the external service provider only. Therefore, processing of personal data by ECDC is limited to storing ticket numbers without any names / personal identifiers attached.

3. Legal analysis

3.1. Prior checking

The processing operation under review presents similarities to two types of processing operations which have been subject to Guidelines issued by EDPS. Firstly, the personal data processed in the current case are health data and administrative data relating to health. Therefore, the Guidelines concerning the processing of health data in the workplace are applicable[1]. Secondly, the processing operation performed by the contractor is similar to the informal procedure typical for the cases of harassment, which is subject to the Guidelines on anti-harassment procedures[2]. Therefore, this Opinion will focus on those aspects that diverge from the Guidelines, need improvement or otherwise merit explanation. The particularities of the current facts reside mainly in the existence of the external contractor that processes data related to the psychological health of the data subjects.

3.2. Lawfulness

EDPS finds that the processing operation is lawful under Article 5(a) of the Regulation.
However, considering the sensitive nature of the data processing operation in question, the EDPS recommends that the controller further details the modalities of the counselling services procedure in more specific rules (policy, communication, decision), applicable to their internal staff[3].

3.3. Processing of special categories of data

We note that all data processed by ECDC in the context of the counselling service are data related to health. The processed health data include both i) medical data (e.g. doctor referrals and prescriptions, medical examination reports) - the data processed by the contractor, and ii) administrative and financial data relating to health (e.g. medical appointments scheduling, invoices for healthcare service provision, indication of the number of days of sick leave, sick leave management)[4] - the data processed directly by ECDC.

---

[1] *Guidelines concerning the processing of health data in the workplace by Community institutions and bodies*, adopted in September 2009 and 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).

[2] See in this regard *Guidelines concerning the processing of personal data during the selection of confidential counsellors and the informal procedures for cases of harassment in European institutions and bodies*, adopted in February 2011 (available at https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Guidelines/11-02-18_Harassment_Guidelines_EN.pdf).

[3] Idem, p. 4.

[4] See *Guidelines on health data*, cited above, p. 2.

Considering that the notification refers in several points to the fact that ECDC is not directly processing personal data[5], it should be clarified that the ticket numbers processed by ECDC and assigned to staff members who seek counselling are "personal data". According to Article 2(a) of the Regulation, personal data mean any information related to an identified or identifiable natural person, while an identifiable person is defined as "*one who can be identified directly or indirectly, in particular by reference to an identification number (...)*". In this case, the data subject can be identified if the records of ECDC are confronted with the records of the contractor. We welcome, as a good practice, the assignment of unique numbers to staff members in the context of data processed for administrative purposes related to the counselling service, so that not all the individual handlers of these data can identify the person seeking counselling. However, they are personal data and are subject to the same safeguards as information referring to an identified person.

3.4. Controllership and attribution of responsibilities

ECDC is the controller of the data processing operation under review, being therefore responsible for its lawfulness, including for compliance with data quality, conservation, transfers, information, rights of the data subject and security requirements.

According to Article 23(1) of the Regulation, "where a processing operation is carried out on behalf of the controller, the latter *shall choose a processor providing sufficient guarantees in respect of the technical and organisational security measures* required by Article 22 and ensure compliance with those measures". In addition, according to Article 23(2), "the carrying out of a processing operation by way of a processor shall be governed by a contract or legal act binding the processor to the controller". This is the case for the processing operation under review, for which a contract has been concluded between ECDC and the processor.

We welcome the fact that the contract enshrines the data security obligations under Article 22 of the Regulation, and the obligation of the processor to act only under the supervision of the controller.

For the sake of clarity, it must be noted that the contract should not refer to the rights of the individuals representing the contractor in their quality of "data subjects", stemming from Regulation 45/2001 (see Articles 11.6.2 and 11.6.3 of the contract). In this regard, it suffices that the persons working for the controller are informed, in line with Articles 11 and 12 of the Regulation, about the details of the processing operation that may involve the processing of their personal data.

In addition, we recommend the insertion of a clause expressing the obligation for the processor to inform the controller if it intends to subcontract the processing and the requirement that the contractor shall not subcontract any of its processing operations without the prior approval of the controller.

3.5. Rights of the data subject

The data subject has the right of access (Article 13 of the Regulation) and the right to rectification (Article 14). ECDC indicated in the notification, under the section about "procedures to grant rights of data subjects", that "no data concerning individuals is collected

[5] See points 5, 6, 8, 10 of the notification.

by ECDC". The electronic information about tickets is personal data (see section 3.2 above), therefore the data subjects must be granted the rights to access and rectification.

3.6. Information to the data subject

Pursuant to Articles 11 and 12 of the Regulation, those who collect personal data are required to inform individuals that their data are being collected and processed. Individuals are further entitled to be informed of *inter alia* the purposes of the processing, the recipients of the data and the specific rights that individuals, as data subjects, are entitled to.

The information about the data processing under review is available on the intranet and sent by the ECDC on 29 August 2014 cannot be considered as a "Privacy Notice" in the sense of Articles 11 and 12 of the Regulation. The information provided concerns the purpose of counselling in general, the procedures to make appointments and the address of the clinic and directions to get to the clinic. The phrase referring to confidentiality does not suffice to consider that the requirements of providing information to the data subject are met.

We recommend that the ECDC adopts a Privacy Notice in compliance with Articles 11 and 12 of the Regulation in order to guarantee a fair and transparent processing regarding such sensitive processing in respect of the staff members' rights.

We welcome the fact that the available information is on the intranet and we recommend that the Privacy Notice is published as well on the intranet. In addition, we recommend that the staff members are informed about the processing operation in case of a request for counselling services to the person concerned, when appropriate before the processing begins[6]; for instance, at the time they approach the in-house doctor or the HR department to obtain the ticket number for the appointment for counselling.

Finally, we point out that the general rule remains direct access with regard to the right of access of the data subject to the medical file processed directly by the contractor. However, *ex* Article 20(1)(c) of the Regulation, the access to data of **psychological or psychiatric nature** can be provided *indirectly*, 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 at stake[7].

3.7 Conservation of data

According to the notification, the ECDC keeps the electronic information about tickets (such as identification numbers, date of issue, date of return as supporting document for invoicing) for budgetary purposes and audit trail of financial purposes. ECDC informed the EDPS that "no personal data appears on the tickets; hence no retention period has been considered specifically for this data".

Having regard that the persons to whom the tickets were attributed are identifiable, and the tickets are personal data, we recommend the ECDC to establish a retention period, in compliance with Article 4(1)(e) of the Regulation.

[6] See in this regard *Guidelines for anti-harassment procedures*, cited above, section 7.
[7] See *Guidelines on processing health data*, cited above, section 6.

Conclusion:

There is no reason to believe that there is a breach of the provisions of Regulation (EC) 45/2001 provided that the considerations in this Opinion are fully taken into account. In particular, the ECDC should:

1. Further detail the modalities of the counselling services procedure in more specific rules (policy, communication, decision), applicable to their internal staff;
2. Amend the contract with the service provider, so that a clause is introduced to express the obligation for the processor to inform the controller if it intends to subcontract the processing and the requirement that the contractor shall not subcontract any of its processing operations without the prior approval of the controller;
3. Exclude from the contract the references to the rights of the "contractor" stemming from the Regulation (see parts of Articles 11.6.2. and 11.6.3 of the contract);
4. Grant rights to access and rectification to the data subjects for the personal data ECDC directly processes;
5. Adopt a Privacy Notice in compliance with Articles 11 and 12 of the Regulation and make sure that staff members are informed about the details of the processing operation at the time they approach the in-house doctor or the HR department to require access to counselling.
6. Establish a retention period for the data the ECDC directly processes, in compliance with Article 4(e) of the Regulation.

Done at Brussels, 22 April 2016.

(**signed**)

Wojciech Rafał WIEWIÓROWSKI