Opinion on a notification for Prior Checking received from the Data Protection Officer of the European External Action Service regarding the "activity of the mediation service"

Brussels, 25 March 2014 (2013-0518)

1. Proceedings

On 17 May 2013 the European Data Protection Supervisor (**EDPS**) received a notification for prior checking under Article 27(3) of Regulation (EC) No 45/2001 (the Regulation) relating to the processing of personal data in the course of the "activity of the mediation service" from the Data Protection Officer (**DPO**) of the European External Action Service (EEAS).

Annexed to the notification were the mandate of the mediator, a privacy statement and Commission Decision (EC) 2006/1624 on the dignity of the person and preventing harassment.

Questions were raised on 31 May and 25 July 2013 to which the EEAS replied on 18 July and 14 August 2013, including an updated version of the notification. On 31 October, the EDPS requested a meeting to discuss the case, which took place on 8 November 2013. The draft Opinion was sent to the DPO for comments on 19 December 2013. The EDPS received a reply on 14 February 2014, which was discussed at a meeting on 25 February 2014.

As this is an *ex-post facto* prior check, meaning that the processing operation was already in place at the time of notification, the deadline of two months for the EDPS to issue his Opinion does not apply. The case has been dealt with on a best-effort basis.

2. The facts

The EEAS has established a mediation service to deal with cases submitted by staff members or departments of the EEAS. Cases can relate to a variety of conflicts in the workplace, for example relating to individual decisions of the administration, or dissatisfaction with the work environment or work conditions, but also psychological and sexual harassment. The mediation service is supposed to act as a facilitator and conciliator, but has no decision-making power of its own. Its mandate is established by the Chief Operating Officer. The activities of the mediation service should be distinguished from those of the confidential counsellors, notified separately and dealt with under case number 2013-0957.

The controller is referred to in the notification as the mediator of the EEAS *ad personam*, with the mediation service's law officer mentioned as "delegated controller".

Potential data subjects are all persons working for the EEAS -headquarters and in delegations-, irrespective of their status or contract, which fall into one of the three categories below:

- persons who contact the mediation service ("persons in difficulty");
- persons complained against;
- witnesses and other persons involved in the case.

When dealing with cases, the mediation service collects a wide range of personal data, such as identification and contact details of persons involved, nature of the problem, case history, type of intervention, contacts with other departments, results of interventions, messages to and from persons involved in the case. These data may include data falling under the special categories of Article 10. Files are collected and stored both on paper and electronically. The content of paper and electronic files is not always the same; the case file is the sum total of paper and electronic files.

Persons contacting the mediation service are informed about the processing via a privacy statement when contacting the mediation service. The privacy statement is also available on the EEAS intranet. According to the notification, persons complained against will be informed "if and when deemed appropriate". Any contact between the mediation service and the person complained against is subject to the prior consent of the person in difficulty.

Data subjects can exercise their rights by contacting the controller; a contact point is provided in the privacy statement. The EEAS will react to requests within 15 days; where justified, rectifications or deletions will be performed within one month. The privacy statement notes that the right of access may be restricted.

The notification notes that transfers without prior consent of the person in difficulty may only "*occur in exceptional cases covered by Article 20(1) c) and e) of Regulation 45/2001, for example when necessary to ensure the protection of a member of staff concerned*".

Cases are closed when either a friendly solution is found, or when the process moves on to a formal stage (e.g. disciplinary proceedings, Article 90(2) complaints, or litigation). Both paper and electronic files are kept for five years after the closure of a case. In case of on-going judicial proceedings, this term may be expanded for another five years. Following this period, anonymous information may be kept for statistical purposes. How the data will be anonymised is not defined yet.

[...]

3. Legal analysis

3.1. Prior checking

The processing of data constitutes a processing of personal data ("*any information relating to an identified or identifiable natural person*" - Article 2 (a) of the Regulation), carried out by a Union body in the exercise of activities which fall within the scope of Union law.[1] The processing of the data is done partly through automatic means. Therefore, the Regulation is applicable.

Article 27 (1) of the Regulation subjects to prior checking by the EDPS all "*processing operations likely to present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes*". Article 27 (2) of the Regulation contains a list of processing operations that are likely to present such risks.

[1] Following the entry into force of the Lisbon Treaty, the references to "Community institutions" and "Community law" in the Regulation should be read as "Union institutions" and "Union law".

Article 27(2)(a) mentions processing operations that involve data relating to health and to suspected offences and several other special categories (Article 27(2)(a). Such data may possibly be processed in the mediation service's activities.

Article 27(2)(b) additionally mentions processing operations intended to "evaluate personal aspects relating to the data subject", which is the case here.

The activities of the EEAS mediation service are thus subject to prior checking by the EDPS.

Since prior checking is designed to address situations that are likely to present certain risks, the Opinion of the EDPS should be given prior to the start of the processing operation. In this case however the processing operation has already been established. In any case, this is not an insurmountable problem in that any recommendations made by the EDPS may still be adopted accordingly.

The notification of the DPO was received on 17 May 2013. On 31 May and 25 July 2013, the EDPS raised questions, to which the EEAS replied on 18 July and 14 August 2013. On 31 October, the EDPS requested a meeting to discuss the case, which took place on 8 November 2013. The draft Opinion was sent to the DPO for comments on 19 December 2013. The EDPS received a reply on 14 February 2014, which was discussed at a meeting on 25 February 2014.

3.2. Lawfulness of the processing

Under Article 5(a) of the Regulation, processing that is "*necessary for performance of a task carried out in the public interest on the basis of the Treaties establishing the European Communities or other legal instruments adopted on the basis thereof*" is lawful. Recital 27 adds that this includes "*processing necessary for the management and functioning of those institutions and bodies*".

The mandate of the mediator, which is established by a Decision of the Chief Operating Officer, sets out the tasks of this service. The notification and privacy statements also make reference to the European Commission's policy on protecting the dignity of the person and preventing psychological and sexual harassment, which was made applicable to the EEAS by a decision of the Chief Operating Officer. The notified processing is part of a policy aiming to prevent conflicts at work, based partly on Article 12a of the Staff Regulations (prohibition of harassment), Article 11 of the Conditions of employment for other servants, Article 1d (prohibition of discrimination) and Article 24 (protection of staff). The notification also refers to Articles 86 (disciplinary measures) and 90 (appeals) of the Staff Regulations. The EDPS would like to point out that the latter two Articles refer to well-established formal procedures; the character of the mediator's tasks is decidedly different and cannot be covered under these formal procedures. The notification should be adapted accordingly.

Nonetheless, the decision of the Chief Operating Officer establishing the mediator's mandate provides a proper legal basis; the processing is thus lawful under Article 5(a) of the Regulation. Article 5(d) (consent of the data subject) is difficult to use as well, since it's the consent of the data subject that is needed here -while it could serve as a supplementary ground for lawfulness concerning data of persons in difficulty, it will likely not work for persons complained about. Article 5(e) (vital interests of the data subject) can be a supplemental ground for lawfulness in specific cases.

Recommendation: Adapt the information on lawfulness and legal basis of the processing according to the explanations in the section above.

3.3. Controllership

Article 2(d) defines the "controller" as the "institution or body, the Directorate-General, the unit or any other organisational entity which alone or jointly with others determines the purposes and means of the processing of personal data".

In the notification, the controller is referred to as the mediator of the EEAS *ad personam*, with the mediation service's law officer mentioned as "delegated controller".

From a legal perspective, the EDPS considers the EEAS as organisation as controller. The EDPS would also like to point out that the responsibilities of the controller always rest with the controller -while of course the actual processing will be carried out by certain staff member and indicating a contact person is a good practice, the controller retains its responsibilities. In this sense, the EPDS considers the two staff member indicated as (delegated) controller to be the contact points.

3.4. Processing of special categories of data

Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and data concerning health or sex life is in general prohibited. Exceptions are contained in Article 10(2) and 10(3).

Concerning special categories of data relating to persons in difficulty submitted by them, the specific rights and obligations of the controller in the field of employment law (Article 10(2)(b)) can be such an exception. In any case, the EEAS should ensure that such data are only included in the case file when they are indispensable for carrying out the tasks of the Mediation service, also taking into account the fact that the person submitting the information may not be the person referred to.

Recommendation: ensure that special categories of data are only included in the case file when they are indispensable for carrying out the tasks of the Mediation service.

3.5. Data Quality

Data must be adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed (Article 4(1)(c)).

Given that the circumstances of each case differ, there is no definite list of data categories that can be established beforehand. Persons dealing with cases should thus be informed about this principle; only data that are adequate, relevant and not excessive in relation to the specific case at hand should be processed. Similarly, whenever personal data are communicated, due care should be taken to limit the amount communicated and to safeguard the data subject's interests.

The principle of data quality also contains the requirement that data must accurate and where necessary kept up to date (Article 4(1)(d)). Data subjects have the right to access and the right

to rectify their data, so that the file can be as complete as possible. This also makes it possible to ensure the quality of data.

Recommendation: ensure that only data that are adequate, relevant and not excessive in relation to the purpose are processed.

3.6. Conservation of data

As a general principle, personal data must not be kept in a form which permits identification of data subjects for longer than is necessary for the purpose for which the data are collected and/or further processed. Further storage for historical, scientific or statistical use is possible under certain conditions (Article 4(1)(e) of the Regulation).

According to the notification, the mediation service stores case files for five years after their closure. Afterwards, they are anonymised and kept for statistical purposes. How the data will be anonymised is not established yet.

Article 4(3) of the mediator's mandate establishes that "*a brief record of the cases dealt with, the solutions proposed and the outcome of the mediation process*" shall be kept for five years after the closure of a case.

The EEAS maintains that it is necessary to continue storing the full files for this period, noting that it was not uncommon for cases to be re-opened. This period is similar to the one established by the Commission's mediation service[2]. Given that the mediator's files are only to be used for mediation and thus are subject to a strict purpose limitation, this can be accepted.

Concerning further storage for statistical purposes, the EEAS should ensure that the data are properly anonymised. The current practice of storing the entire case file also makes anonymisation more difficult, given that even if names are removed, other elements in the files (unit, position, etc.) might still allow for indirect identification of data subjects. Having a standardised closure form would provide a better basis for effective anonymisation and could contain all items of information needed for statistical purposes (kind of conflict, outcome, etc.).

Recommendation: Ensure that data stored for statistical purposes are properly anonymised.

3.7. Transfer of data

Article 7 of the Regulation allows transfers within and between institutions subject to the Regulation when they are "*necessary for the legitimate performance of tasks covered by the competence of the recipient*".

Transfers are only foreseen within the EEAS and to services responsible for Commission staff in delegations, and only if and to the extent this is necessary to fulfil the service's mediation mandate (see also Article 2(10) of the mediator's mandate). The privacy statement also mentions that such transfers will only occur with the consent of the data subject as an additional safeguard (see also Article 2(13) of the mediator's mandate). In any case, in order

[2] See case 2009-0010.

to safeguard the confidential nature of the procedure, transfers should be limited to the minimum amount necessary.[3]

Recipients should be reminded that they can only process the data for the purposes for which they were communicated to them (see Article 7(3) of the Regulation). This could take the form of a standard clause in e-mails or letters transmitting data.

Recommendation: remind recipients that they may only process personal data transferred to them for the purpose for which they were transferred and restrict transfers to the minimum necessary.

3.8. Rights of access and rectification

Article 13 of the Regulation gives data subjects the right to access their own personal data; Article gives them the right to obtain rectification of inaccurate or incomplete data. Restrictions are possible under the conditions set out in Article 20.

Data subjects can exercise their rights by contacting the controller using the functional mailbox. The EEAS will reply to such requests within 15 days and, if it is justified, rectify/erase data within one month. According to the privacy statement, restrictions under Article 20(1) (a) and (c) may apply.

The exceptions in Article 20 should only be used on a case-by-case basis following an evaluation of the individual request. Article 20(1)(c) (rights and freedom of the data subject or third parties) is the most relevant provision here. This concerns especially requests of persons complained against to gain access to the allegations as submitted by the alleged victim.

Recommendation: ensure that restrictions to data subject rights are only applied after a case-by-case examination.

3.9. Information to the data subject

Articles 11 and 12 establish the requirements regarding the information of data subjects. Restrictions are possible in line with Article 20.

A privacy statement containing all necessary information is available on the EEAS intranet.

It will be provided to persons in difficulty contacting the mediation service. According to the notification, "if and when deemed appropriate", it will also be provided to other persons involved in the procedure.

The notification mentions that restrictions under Article 20(1) (c) and (e) may be applied. Article 20(1)(c) may be relevant in situations where the psychological state of a victim does not permit informing the presumed offender immediately. Article 20(1)(e), on the other hand, does not seem pertinent here. Data subject rights, including the right to information can only

[3] The EEAS maintains that in very exceptional situations, transfers may also be necessary without consent, e.g. to ensure the protection of a member of staff. The reference made to Article 20 in the notification form is not necessary here - Article 20 allows restricting data subjects rights, e.g. on access (see section 3.8 below), but has no bearing on the rules on transfers. While consent to the transfer is not necessarily required under the Regulation, it can be a safeguard.

be restricted under the conditions of Article 20 of the Regulation. The relevant case is Article 20(1)(c) (protection of the data subject and rights and freedom of others). This can be the case for informing the person complained against about the procedure. As mentioned above, any contact with such persons is subject to the consent of the alleged victim. As of the point in time when the mediation service contacts the person complained against, there is no further reason to not provide the privacy statement. Similarly, there seems to be no reason to not supply the privacy statements to witnesses who might be contacted in the course of the procedure.

Recommendation: always supply the privacy statement to persons complained against and witnesses when they are contacted by the mediation service.

3.10. Security measures

[…]

4. Conclusion

There is no reason to believe that there is a breach of the provisions of Regulation 45/2001 providing that the recommendations made in this Opinion are fully taken into account. To recall, the recommendations can be summarised as follows:

- adapt the information on lawfulness and legal basis of the processing according to the explanations in section 3.2;
- ensure that only data that are adequate, relevant and not excessive in relation to the purpose are processed;
- ensure that data stored for statistical purposes are properly anonymised;
- remind recipients that they may only process personal data transferred to them for the purpose for which they were transferred and restrict transfers to the minimum necessary;
- ensure that restrictions to data subject rights are only applied after a case-by-case examination;
- always supply the privacy statement to persons complained against and witnesses when they are contacted by the mediation service.

Done at Brussels, 25 March 2014

(signed)

Giovanni BUTTARELLI