Opinion on a notification for prior checking received from the Data Protection Officer of the Committee of the Regions regarding 'psychological and sexual harassment in the workplace (anti-harassment procedure)'

Brussels, 6 October 2010 (Case 2010-0485)

1. Procedure

On 25 June 2010, the European Data Protection Superior (EPDS) received a notification within the meaning of Article 27(3) of Regulation (EC) No 45/2001 (hereinafter 'the Regulation') sent by the Data Protection Officer (DPO) of the Committee of the Regions regarding the Committee's 'anti-harassment procedure'.

Further information was requested on 23 July 2010 and replies were submitted by the DPO on 30 July 2010. A second question was raised by the EDPS on 30 July and replied to on 3 August 2010. The draft Opinion was sent to the DPO for comments on 14 September 2010. The comments were received on 5 October 2010.

2. Examination of the case

Purpose of the processing

The Committee of the Regions plans to introduce a policy to combat psychological and sexual harassment within the institution. This policy is divided into two separate procedures, an informal and a formal procedure. The informal procedure relies essentially on a network of people known as 'persons of trust' who, where mediation becomes necessary, form an ad hoc panel.

This present analysis is therefore concerned firstly with the selection of the persons of trust and secondly with the informal policy outlined by the Committee. As for the formal procedure, this falls within the broader scope of the Committee's administrative investigations (case file 2007-382).

The processing of data is based on Article 1(d), Article 12(a) and Article 24 of the Staff Regulations and also Article 11 of the Conditions of Employment of Other Servants. A draft decision concerning psychological and sexual harassment in the workplace within the Secretariat-General of the Committee of the Regions has therefore been drafted on this basis.

The selection of the persons of trust

These persons are selected by means of a call for applications. The Selection Committee is chaired by the Director of Administration and includes amongst others a member appointed by the Personnel Committee. In addition to the administrative data contained in the application form, the Committee will take into account personal aspects and the motivation, the abilities and the availability of the applicants and will, as far as possible, endeavour to strike a balance between genders and function groups together with a representative selection from the institution's different services. On the basis of the work done by the Committee, the Appointing Authority will then appoint the persons selected as persons of trust. A list of the persons selected and their professional contact details will then be published on the Committee's Intranet. The selection files (application forms and supporting documents) will be retained for one year after the procedure has been completed. On launching a call for applications which will be in the form of a Staff Notice, the Committee proposes to provide applicants with information about the rules governing the selection procedure. The call for applications will also include information about the terms and conditions applying to the processing of data in this context. Applicants will have the right of access to and the right to rectify their personal data. The mandate of persons of trust is for a period of three years, and it is renewable.

The informal policy

All persons who work for the Committee may be involved, whatever their status or type of employment contract: persons consulting a person of trust, the persons complained of by them and witnesses or other persons involved.

Persons who consider that they have suffered harassment may raise the matter with their immediate superior, or a person of trust (see above) or a panel of persons of trust.

Except in urgent situations, where the immediate superior is consulted, the information given by the alleged victim is considered to be confidential.

When consulted, the person of trust may record the name of the person involved and the dates of their consultations. With the written consent of the person consulting him/her, the person of trust may also take notes and receive documents considered relevant to the case.

The panel will usually be consulted where there is a wish for mediation between the alleged harasser and the alleged victim, at the request of either of them. Following a referral for mediation, the panel may, where appropriate make recommendations or even draw the Appointing Authority's attention to the existence of a dysfunctional situation within the service (in recurring cases). In order to perform its tasks, the panel may call upon an outside expert where the complexity of the case justifies this and with the prior consent of the parties concerned. Where the alleged victim in the first place consults a person of trust, the latter will refrain from sitting on the panel dealing with the same case.

The following personal data may be processed as part of this process: identification data (name, date of birth, address, telephone number, grade etc.); administrative data (grade, service(s), functions and responsibilities etc.); claims, statements, information concerning the case in question given by the victims, the subjects of the complaint, witnesses or other persons involved in other capacities; the dates of consultations with a person of trust and the

stages in any possible mediation procedure. Where the victim has given his/her written consent, the person of trust may take notes during a consultation and also receive documents which the former may wish to give, provided that the person of trust considers this necessary in order to perform his/her duties. Special categories of data, within the meaning of Article 10 of the Regulation, may be processed. In the case of harassment, these may more particularly involve data referring to personal health or sex life.

Administrative data may be extracted from electronic databases, but the actual processing will be manual, as the files will be in paper format.

Harassment files held by the persons of trust, the chairman of the panel or the immediate superior responsible for a case will be retained for five years. This period covers the time necessary for the persons of trust to complete the mandate for which they were appointed and in particular the follow-up and evaluation of the anti-harassment policy being implemented. This period of time is also designed to enable potential recurrent cases to be identified with a view to their prevention. Files are retained for an additional five years where, at the date of expiration of the initial five years, there are ongoing legal or administrative proceedings which may necessitate their consultation (for example an action for damages, a request by the Ombudsman, a referral to the Civil Service Tribunal).

Once they have been rendered anonymous, personal data shall be then used for statistical purposes (with the express aim of following up and evaluating the implementation of the anti-harassment policy).

According to the notification and the documents received from the Committee, if the administration and more specifically the working conditions/rights/training unit is the formal controller, the procedure is conducted in such a way that, in practice, other bodies/persons share the role of controller. In fact, the persons of trust, the panel or the immediate superior involved will process the data directly and will treat them as confidential. The purpose of the informal procedure is to provide the alleged victim and the other persons involved with a forum at which they may express their views in complete confidence. The relevant data which are likely to be processed are therefore in practice processed by these three persons/bodies and not by the administration, which here simply provides administrative support for the procedure (selection of persons of trust, statistics).

In urgent situations, data may be forwarded to the Appointing Authority where precautionary measures need to be taken in the interests of the persons concerned and of the service. Under the formal procedure, an investigation may result in data being communicated to the Appointing Authority/AECE, their advisors, the Disciplinary Board, the recruitment and careers unit, the working conditions/rights/training unit, the Civil Service Tribunal, the Court of Justice, the Ombudsman, the Legal Service and, in the case of investigations involving members of staff of two Committees, the Appointing Authority/AECE of the other institution.

Members of staff have the right to access their personal data and also the right to rectify any inaccurate or incomplete personal data. Data subjects may, as appropriate, contact the person of trust, the chairman of the panel or their immediate superior in order to obtain rectification of inaccurate data contained in documents relating to them.

For general purposes, a declaration of confidentiality relating to the formal and informal procedures will be available on the Committee's Intranet. This draft declaration has also been submitted to the EDPS.

In this declaration, data subjects are informed of: the identity of the controller, the purposes for which the data will be processed, the recipients of the data, the period for which the data will be retained, their right of access and their right of recourse to the European Data Protection Superior.

More specifically, an alleged harasser will be informed that the alleged victim has contacted a person of trust (or the panel or his/her immediate superior) only where the latter has given his/her consent. In a case where, on expiry of the mandate of the person of trust, the alleged victim still refuses to allow the subject of the complaint to be informed of the steps he/she has taken, any data relating to that person will be removed and no information allowing him/her to be identified will be retained.

The Committee has put security measures in place, in particular with regard to data confidentiality.

3. The legal aspects

3.1. Prior checking

Applicability of the Regulation: The anti-harassment policy within the Committee of the Regions involves the processing of personal data ('any information relating to an identified or identifiable person' – Article 2(a) of the Regulation).The data processing in question is carried out by a European Union (formerly 'a Community') institution and is carried out in the exercise of activities which fall within the scope of European Union (formerly 'Community') law. The data are processed manually, but their content will form part of a structured computer file; a personal file relating to application forms from persons of trust and a file for each case of harassment, whether it be retained by the person of trust, the panel or the person's line manager. Article 3(2) is therefore applicable in this case. Consequently, Regulation (EC) No 45/2001 is applicable.

Justification for the prior checking: Article 27(2) of the Regulation lists the processing operations likely to present risks, making them subject to prior checking by the European Data Processing Superior. This list includes Article 27(2)(b): 'processing operations intended to evaluate personal aspects relating to the data subject, including his or her ability, efficiency and conduct'). The procedure for the appointment of persons of trust clearly involves a part concerned with the evaluation of the applicants' abilities. The harassment files also contain information relating to the conduct of the data subjects (the alleged harasser for example). Article 27(2)(a) refers to 'processing of data relating to health and to suspected offences, offences, criminal convictions or security measures'. In the case under examination, data relating to health, where the mental health of the data subject is at stake, could for example be processed. For all these reasons, the processing of data connected with the anti-harassment policy is 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 EPDS should be given prior to the start of the processing operation. Any recommendations made by the EPDS must be fully taken into account.

Time limits: the notification from the DPO was received by post on 8 July 2010 (an electronic version was received on 25 June 2010). According to Article 27(4) of the Regulation, the EPDS must deliver his/her Opinion within two months following receipt of a notification. The procedure has been suspended for a total of 29 days. Thus, this Opinion should be delivered not later than 8 October 2010.

3.2. Lawfulness of the processing

The lawfulness of the processing must be examined in the light of Article 5(a) of the Regulation, which states that 'processing is necessary for the 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. The selection of persons of trust and the informal policy are essential elements put in place by the Committee for the purpose of combating psychological and sexual harassment within the institution. This public interest task is essentially based on Article 12(a) of the Staff Regulations (the legal basis for the processing of the data), which requires officials to refrain from any form of psychological or sexual harassment. Lastly, once it is adopted, the Draft Decision on psychological and sexual harassment in the workplace will provide an additional basis for the processing in question.

The legal basis is therefore appropriate and the requirements of Article 5(a) appear to be fulfilled.

3.3. Processing of special categories of data

The processing of personal data during the course of a procedure may require the processing of special categories of data, such as those described in Article 10 of the Regulation, such as for example data concerning health or sex life.

The processing of such data may become necessary as part of the informal procedure in order to comply with the specific rights and obligations of the controller in the field of labour law, insofar as it is authorised by legal instruments based on the Treaty (Article 10(2)(b) of the Regulation). In fact, the legal basis referred to above shows that the institution, as an employer, has the duty to ensure that the working environment is free from any form of psychological or sexual harassment. On that basis, the processing during that procedure of sensitive data, relevant to the case in question and proportionate to the aim being pursued can be justified.

3.4. Data quality

Personal 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)). As regards the selection of persons of trust, the data collected appear to comply with Article 4(1)(c).

In the case of the informal procedure, this is an essential point. A distinction needs to be made between two types of data: 'hard' or objective data – this may include administrative or identification data – and 'soft' or subjective data, which include claims/statements made by the persons involved, since they are based on the subjective perception of individuals. This distinction will also be useful when it comes to analysing the data subject's rights of access and rectification (see Section 3.7. below).

The Committee should define and structure the collection of 'objective' data so as to avoid any excessive collection of data. For example, once they have been rendered anonymous, the Committee of the Regions intends to retain certain data for longer periods for statistical purposes. It is clear that, if these data are to be useful, they have to be determined in advance. When deciding on the type of data to be retained, the Committee should take particular care to ensure the 'anonymity' of the data. In fact, certain anonymous data, when cross-referenced (statistical inference) can easily reveal an individual's identity.

On the contrary, it is not possible to determine in advance which 'subjective' data should be collected. These data depend on the case in question. However, this collection should be governed by the principle laid down in Article 4(1)(c). The persons involved should be reminded of the principle concerning the need for the data.

In addition, data must be 'processed fairly and lawfully' (Article 4(1)(a) of the Regulation). The lawfulness of the data has already been analysed in Section 3.2. of this Opinion. As regards fairness, this concerns the information to be given to the data subject (see Section 3.8. below).

Personal data must also be 'accurate and, where necessary, kept up to date'. The Regulation also stipulates that 'every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified' (Article 4(1)(d)). In principle, the system described will help to ensure that data are accurate and kept up to date, given that the data subject has the possibility of accessing the data by contacting the person holding them and of exercising the right to rectify them.

However, it should be pointed out that the accuracy of 'subjective' data is not measured by the fact of communication by the data subject, but rather by the accuracy with which the data subject has communicated the information. Thus, the data subject's right of access and rectification permits him/her her to assess whether the data retained indeed represent the statements/allegations made. In this context, the requirement concerning the accuracy of the data therefore means that the person collecting them must make sure that statements/allegations made by individuals are clearly indicated as such and not as established facts. This is particularly important in the case of the transfer of data.

For a full analysis of these two rights, see Section 3.7. *infra*.

3.5. Retention of data

Article 4(1)(e) of the Regulation establishes the principle that personal data must be 'kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which they were collected or for which they are further processed'.

As a reminder, in order to keep a record of cases dealt with under the informal procedure, files are retained for five years. They are retained for a further five years if, at the date of expiration of the initial five years, there are ongoing legal or administrative proceedings which may necessitate their consultation. As for the persons of trust' application forms and supporting documents, they are retained for one year after the file has been closed. The EDPS considers that these retention periods are compatible with Article 4(1)(e).

Regarding data kept for longer periods for statistical purposes, the EDPS recommends that the greatest care be taken to render those data anonymous. The retention of data for statistical purposes must be carried out in accordance with Article 4(1)(e) (see also the section on data quality above).

3.6. Transfer of data

The processing of data in this context needs to be examined in the light of Article 7(1) of the Regulation. This processing concerns the transfer of personal data within or to other Community institutions 'if the data are necessary for the legitimate performance of tasks covered by the competence of the recipient'.

Transfers of data carried out in connection with the selection of persons of trust appear to meet this criterion.

As a reminder, under the informal procedure, in urgent cases, data are transferred to the Appointing Authority/AECE in order to enable the latter to take any precautionary measures which may be necessary. Regarding such transfers, we would point out that only relevant data may be transferred. Such transfer is therefore entirely lawful insofar as its purpose is covered by the competence of the recipients. Article 7(1) has therefore been complied with.

The Committee of the Regions must also ensure that the recipients process those data exclusively for the purposes for which they were transferred, that is to say, to combat harassment. This principle is particularly important in view of the sensitivity of the data in question.

3.7. Right of access and rectification

Article 13 of the Regulation deals with the right of access – and rules thereon – of data subjects, on their request, to data being processed which concerns them. Article 14 deals with data subjects' right of rectification. The processing under examination here is said to guarantee those two rights.

As a reminder, the general rule applied implies access to personal data concerning the data subject held in a file. The application of this rule may be restricted where that access may compromise the data subjects' protection or the rights and freedoms of others, which should be decided on a case-by-case basis and never automatically.

Article 20 of the Regulation in fact provides for certain restrictions on the right of access, in particular where such restriction constitutes a necessary measure to *'(…); c) safeguard the protection of the data subject or the rights and freedoms of others'*.

In the case under examination here, the persons involved may experience a restriction of their right of access. In fact, access is conditional upon their being informed by the person of trust (the panel or their line manager), following the complainant's consent, that an informal procedure concerning them is underway (see Section 3.8.). In addition, the transfer of data may not negatively affect one of the parties involved in the case, the smooth running of procedures or future relations between the parties.

In any event, the Committee must take account of and comply with Article 20(3): *'If a restriction provided for by paragraph 1 is imposed, the data subject shall be informed, in accordance with Community law, of the principal reasons on which the application of the restriction is based and of his or her right to have recourse to the European Data Protection Superior'*. Regarding the right to be informed, this provision should be read in conjunction with Articles 11, 12 and 20 of the Regulation (see Section 3.8.).

In addition, account should also be taken of Article 20(4): *'If a restriction provided for by paragraph 1 is relied upon to deny access to the data subject, the European Data Protection Superior shall, when investigating the complaint, only inform him or her of whether the data have been processed correctly and, if not, whether any necessary corrections have been made.'*. The right of indirect access must be guaranteed in the present case. In fact, this provision will for example play a role where the data subject has been informed that data concerning him/her have been processed or is aware of this, but where his/her right of access remains restricted having regard to Article 20.

Article 20(5) states that: *'Provision of the information referred to under paragraphs 3 and 4 may be deferred for as long as such information would deprive the restriction imposed by paragraph 1 of its effect'*. It may prove necessary for the Committee to defer the provision of such information in accordance with this provision in order to protect the presumed victim.

3.8. Information to be given to data subjects

The provisions of Article 11 of Regulation (EC) No 45/2001 (Information to be supplied where the data have been obtained from the data subject) concerning the information to be given to the data subject are applicable in the present case. The same will apply to the provisions of Article 12 (Information to be supplied where the data have not been obtained from the data subject), since information may be obtained from other sources, including the complainant in the case of a complaint being made about a person.

As a reminder, in the case under examination here, the information is given in general terms via a declaration of confidentiality available on the Committee's Intranet. This general information concerning the processing of data covers the various items listed in Articles 11 and 12 of the Regulation, apart from the legal basis. Regarding the reference to the right of access, the declaration should contain a reference to the right of access and the right of 'rectification' and not of 'verification' as it does at present.

Information must also be provided specifically, firstly to the person who has complained of harassment (when the informal procedure is started, by the person of trust, the person's immediate superior or the panel) and to the subject of the complaint (provided that the data subject has given his/her consent).

Article 20 of the Regulation referred to above (see Section 3.7.) provides for certain restrictions of the right to information, for example where such restriction constitutes a necessary measure to *'(…); c) safeguard the protection of the data subject or the rights and freedoms of others'*. In fact, in some cases, it may be necessary not to inform the data subject (in those cases, the person complained of) so as not to jeopardise the smooth running of the procedure. As a reminder, in the case under examination, the persons complained of are informed by the person of trust, with the victim's consent, that an informal procedure concerning them is underway (although exceptions to this are made in order to protect the complainant). Where, when the action taken by the person of trust has been completed, the presumed victim still refuses to permit the person complained of to be informed of the step he/she has taken, any data relating to that person will be removed and no information enabling him/her to be identified will be retained.

In addition, Article 20(5) should be applied in specific circumstances: *'Provision of the information referred to under paragraphs 3 and 4 may be deferred for as long as such information would deprive the restriction imposed by paragraph 1 of its effect.'* (Paragraph 3 provides that the data subject has the right to be informed of the reasons on which the restriction is based and of his/her right of recourse to the EDPS; paragraph 4 provides for an indirect right of access via the EDPS and for the result of that access to be communicated to the data subject).

3.9. Security

According to Article 22 of Regulation (EC) No 45/2001 concerning security of processing, *'the controller shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risks represented by the processing and the nature of the personal data to be protected.'*

On the basis of the information supplied, the EDPS has no reason to believe that the Committee has not implemented the security measures required pursuant to Article 22 of the Regulation.

4. Conclusion

There is no reason to believe that there is a breach of the provisions of Regulation No 45/2001, provided that the following recommendations are taken into account. The Committee of the Regions should, *inter alia*:

- Define and structure the collection of 'objective' data in order to avoid any excessive collection of data;
- Remind the various persons involved (persons of trust, panels, immediate superiors) of the principles set out in Article 4(1)(c) regarding the collection of subjective data;

- Ensure of the quality of data collected for statistical purposes and also that they are rendered anonymous in accordance with Article 4(1)(e);
- Amend the declaration of confidentiality as indicated in Section 3.8.
- Provide ‘specific’ information to data subjects, as described in Section 3.8.

Done at Brussels, 6 October 2010

(signed)

Giovanni BUTTARELLI

Assistant European Data Protection Superior