Opinion on notifications for prior checking received from the Data Protection Officers of certain EU agencies concerning the "*anti-harassment policy*" and "*the selection of confidential counsellors*".

Brussels, 21 October 2011 (Case 2011-0483)

1. Procedure

Since September 2008, the European Data Protection Supervisor (EDPS) has adopted a new procedure for ex post prior checking analysis regarding common procedures within the agencies.

On 21 February 2011, the EDPS sent "*Guidelines concerning the processing of personal data in anti-harassment policy and selection of confidential counsellors*" (EDPS Guidelines) to all EU institutions and bodies including agencies. These agencies were requested to submit the notifications regarding their procedures on the fight against harassment accompanied by a cover letter from the Data Protection Officer (DPO) highlighting the specific aspects vis-à-vis the EDPS Guidelines. The deadline to submit notifications was 29 April 2011. On the basis of a request from certain agencies a two months' extension of the deadline to submit notifications (30 June 2011) was granted by the EDPS. Nine agencies submitted notifications and cover letters:

- European Agency for the Management of Operational Cooperation at the External Borders (**FRONTEX**),
- European Chemicals Agency (**ECHA**),
- European Foundation for the Improvement of Living and Working Conditions (**EUROFOUND**),
- European Food Safety Authority **(EFSA**),
- Translation Centre (**CDT**),
- Office for Harmonization in the Internal Market (**OHIM**),
- European Centre for the Development of Vocational Training (**CEDEFOP**),
- European Monitoring Centre for Drugs and Drug Addiction (**EMCDDA**),
- European Training Foundation (**ETF**).

Some agencies took advantage of the Guidelines to establish their procedure[1].

Some agencies informed the EDPS that they had not yet set up any anti-harassment procedures[2]. Some institutions whose procedures had been already prior checked by the EDPS updated the EDPS in the light of the Guidelines[3]. All other agencies did not reply.

---

[1] **EMCDDA**

[2] **CFCA**, **EDPS, EMSA, EU-OSHA, SESAR Joint Undertaking**

[3] The **ECB** informed the EDPS that the internal notification to the DPO was updated to include stakeholders that may play the same role as the social counsellor emphasising that their conduct must follow the same data

The EDPS reminds the agencies that have not notify their procedure that they should do it prior to the processing of personal data in the frame anti-harassment procedures is put into place, failing that they would be in breach of Regulation (EC) 45/2001 (the Regulation).

The fight against harassment is generally composed of two procedures: (i) the selection of confidential counsellors and (ii) the informal procedure.

The **ETF** underlined in his cover letter that the procedure to select external candidates applies, by analogy, to the selection of counsellors and this procedure had already been prior checked by the EDPS. The **ECHA** does not organise the selection of confidential counsellors, the agency outsources the role of confidential counsellor to an external service provider. The contract with the service provider is analysed in point 2.10.

The draft Opinion was sent to the nine DPOs of the agencies concerned for comments on 26 September 2011. The DPOs' comments were received by 20 October 2011.

2. Legal aspects

2.1. Prior checking

The processing operations under examination are subject to prior-checking in conformity with Article 27(2)(b) of Regulation 45/2001, since they involve (i) an evaluation of the applicants' ability to perform as a confidential counsellor (ii), an evaluation of the conduct of the data subject in case of harassment, and possibly processing operations related to their health. The processing of data relating to health constitutes an additional ground for prior-checking in the light of Article 27(2)(a) of the Regulation.

The EDPS analysed each agency's practice with reference to the data protection principles of the Regulation and evaluated whether each agency followed the EDPS Guidelines or not. In view of the similarities of the procedures, and of similarities presented by some agencies in terms of data protection practices, the EDPS examined all the notifications in the same context and will issue one Joint Opinion. In this Joint Opinion the EDPS highlights any practice which does not seem to be in conformity with the principles of the Regulation or the EDPS Guidelines and provides the agency(ies) concerned with relevant recommendations. Some examples of good practice are also highlighted, where appropriate.

According to Article 27(4) of the Regulation, the EDPS will issue his Opinion within two months following receipt of the notification. Due to the fact that the last notification was submitted to the EDPS on 30 June 2011, the EDPS considers this date as the date of receipt for all notifications. The prior-checking procedure was suspended for a total of 24 days for DPO's and controller's comments. The Joint Opinion must therefore be issued no later than the 24 October 2011 (30 September + August suspension + 24 days of suspension).

.

2.2 Notification

CEDEFOP's notification refers to the *note to the DPO* that was attached to the notification form. As already stated, the notification itself must contain all relevant information. The notification will be published in the EDPS register and therefore references to other documents not available from the register, does not allow proper description of the processing

protection safeguards that the one established for the social counsellors. The **EIB** informs the EDPS that the procedure that was prior checked in 2005 by the EDPS is now under revision.

operation. This applies to several sections of the **CEDEFOP's** notification. The **CEDEFOP** should modify his notification accordingly.

2.3. Lawfulness of the processing

Personal data may only be processed if lawful grounds can be found in Article 5 of the Regulation. The processing operations under examination fall under Article 5 (a), pursuant to which data may be processed if the processing 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* (...)".

It follows that the first issue under Article 5(a) is to determine whether **(i)** there is a specific legal basis for the processing and the second issue is to **(ii)** verify whether the processing of personal data is necessary for the performance of a task carried out in the public interest.

(i) Fight against harassment is based on Article 12 (a) of the Staff Regulations and Article 11 of the Conditions of Employment of Other Servants which prohibits such behaviour. In addition, Articles 1 and 31 (1) of the EU Charter of Fundamental Rights complement the legal basis. The Charter states that every worker has the right to working conditions which respect his or her dignity. The selection of confidential counsellors and the informal procedure are the elements put in place by agencies to combat psychological and sexual harassment.

The fight against harassment is a task carried out in the public interest in the sense of Recital 27 of the Regulation which states: "*processing of personal data for the performance of tasks carried out in the public interest by the Community institutions and bodies includes the processing of personal data necessary for the management and functioning of those institutions and bodies.*" Ensuring working conditions which respect workers dignity forms part of the good management of an EU body.

The Staff Regulations define psychological and sexual harassment and prohibits such behaviour. However, on this basis, the procedure ensuring working conditions free from harassment needs to be developed by each institution or body.

In that regard, the EDPS notes that the **EMCDDA,** the **CEDEFOP,** the **FRONTEX** and the **ECHA** submitted a draft decision (or policy) on their procedure. These agencies should take into consideration all the EDPS recommendations and provide the EDPS with a copy of their draft decision revised accordingly. The **EUROFOUND** submitted his draft policy but underlined that the manual is still being drafted. Once finalised, the manual must be submitted to the EDPS.

The **ETF**, the **CDT** and the **OHIM** have already adopted a Decision on protecting the dignity of the person and preventing harassment. Any recommendations provided by the EDPS in the present Opinion should be duly implemented.

The **EFSA** submitted an old version of his manual and the one currently under revision. Any recommendations provided by the EDPS in the present Opinion regarding the **EFSA** should be duly implemented in the new version of the **EFSA** manual.

(ii) The informal procedure and the selection of confidential counsellors to implement it, necessarily implies the processing of personal data. It follows that the processing of personal

data related to fight against harassment carried out by the agencies under analysis is necessary to perform a task carried out in the public interest according to Article 5 (a) of the Regulation.

2.4. Processing of special categories of data

According to Article 10(1) of the Regulation, "*processing of personal data revealing racial or ethnic origin, political Opinions, religious or philosophical beliefs, trade-union membership, and of data concerning health or sex life, are prohibited*" unless an exception can be found in Article 10 (2) or Article 10 (3).

The **OHIM** and the **CDT** do not mention in the notification that special categories of data might be collected. Their notification should be adapted accordingly. Indeed, the processing of special categories of data can not be excluded during the informal procedure (health data or data concerning sex life in the case of sexual harassment for e.g.). These data can be regarded as necessary for complying with the obligation to fight against harassment, inasmuch as those data are relevant for the case. The same applies to the selection of confidential counsellors who may, when applying for the post, provide for special categories of data.

The **CEDEFOP's** approach is very restrictive towards the processing of sensitive data. According to the notification, neither confidential counsellors nor the coordinator process special categories of data. Retaining such data in the closing form may take place only in exceptional cases. As stated above, the EDPS is of the opinion that in certain circumstances, the confidential counsellor will have to process sensitive data to accomplish his task. The **CEDEFOP** should revise his notification according to this principle. Having said that and in accordance with the data quality principle, the collection of data must follow the data minimisation principle.

2.5. Data Quality

Adequacy, relevance and proportionality
According to Article 4(1)(c) of Regulation 45/2001 *"personal data must be adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed"*.

Informal procedure

The EDPS distinguishes data qualified as "**hard**" or "objective" and data qualified as "**soft**" or "subjective".

The collection of soft data does not follow systematic rules as to the type of data processed; it is not possible to determine a priori the type of data collected. This does not mean that the collection may be random. The data collected by the counsellors must be adequate, relevant and not excessive in relation to the fight against harassment. This analysis must be conducted on a case by case basis by the counsellors.

The **ECHA** outsourced the role of confidential counsellor to an external service provider. The EDPS has received no information as to the instructions provided by the **ECHA** regarding the collection of data and in particular the distinction between hard and soft data and the respect of Article 4. According to Article 23 (2), the processor should act only on instructions from the **ECHA**. Due to the sensitivity of the data, the EDPS would like to know the measures taken by the **ECHA** to ensure that data collected by the provider are adequate, relevant and

not excessive in relation to the purposes of the informal procedure.

It is clear from the notifications from the **OHIM**, the **CDT** and **EUROFOUND** that they only collect adequate, relevant and not excessive data; nevertheless, the EDPS has no information as to how this data quality principle is respected. If existing, draft manual providing instructions (to confidential counsellors for instance) have not been provided to the EDPS. The EDPS would like to be reassured as to the implementation of the data quality principle.

The collection of hard through the forms should allow the identification of recurrent and multiple cases and should not be excessive in relation to that purpose. The **CDT**, the **OHIM**, the **Eurofound**, the **ECHA** did not provide the EDPS with opening and closing forms if any, to allow him to evaluate whether or not the data are relevant and not excessive.

Hard data collected for statistical purposes must be anonymous, in compliance with Article 4(1)(b). The **ECHA** refers to the publication of an annual activity report containing statistics. The EDPS would like to recall that the ability of identifying data subjects might arise for example by means of statistical inferences, especially within small entities; the data collected must therefore be selected cautiously.

Accuracy: Article 4 (1) (d) of the Regulation provides that personal data must be "*accurate and when necessary, kept up to date*". In addition, "*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* ".

Concerning soft data, the requirement of accuracy cannot appertain to the facts themselves (they relate to the subjective perception provided by data subjects). The accuracy therefore refers to the fact that a statement has been made by the data subject and is rightly annotated as such.

In this regard, effective rights of access and rectification of the data subject enable individuals to control whether the data registered reflect the perceptions, statements they wanted to transmit and, in that sense, whether these are accurate and as complete as possible (see therefore point 2.8 on the right to access and rectification below). The **EFSA** took the good initiative to include the accuracy principle into the general privacy statement.

2.6. Transfer of data

The processing covered by Article 7(1) is the transfer of personal data within an EU institution or body or to other EU institutions or bodies which may only take place *"if the data are necessary for the legitimate performance of tasks covered by the competence of the recipient"*.

Whatever the recipient -within or in another EU institution or body- the transfer of data must follow the rules established in Article 7. Article 7.1 provides for strict and cumulative conditions (necessity, legitimate performance of tasks, competence of the recipient) to allow transfer of data.

Article 7 applies without prejudice to Article 5. As mentioned in point 2.3, the processing of data at stake is linked to the performance of a task carried out in the public interest (Article 5

(a) of the Regulation). Accordingly, the use of consent of the individual concerned (Article 5.b) to legitimise the data processing cannot be used as the legal basis for the transfer[4].

The consent in the context of employment is of sensitive nature[5]. Indeed, the consent must be freely given, according to its definition in Article 2(h). The data controller being the employer of the data subject, the data subject may feel himself obliged to give his/her consent.

Furthermore, even if the consent of the data subject was a valid legal basis, the validity of the consent of a person subjected to harassment could be challenged: the strong emotional charge on the alleged victim's shoulders makes any decision related to this experience very difficult.

Article 8 provides also for stringent requirements to transfer data to recipients subject to national law adopted for the implementation of Directive 95/46/EC. Transfer to judicial authorities can only take place if they are *"necessary for the performance of a task carried out in the public interest or subject to the exercise of public authority"* (paragraph a) and transfers to social advisors or psychologists *"if the recipient established the necessity of having the data transferred and if there is no reason to assume that the data subject's legitimate interests might be prejudiced"* (paragraph b). In all scenarios these transfers are exceptional.

It emerges that the confidential character of the informal procedure would be better protected by the safeguards established in Articles 7 and 8 than by consent. It is true however that due to this confidential character of the informal procedure, transfers of data, in particular the notes of the confidential counsellors, should be avoided. The **EFSA**'s new policy on transfers is relatively in accordance with this policy (except for the Opening form, see below).

Finally, the exception foreseen in Article 20(1)(c) applies to the right of access (Article 13) but do not apply to data transfers (Articles 7 and 8).

It seems that there is confusion between the right of access and the transfer of personal data. The first one only applies to someone's own personal data (alleged harasser, alleged victim, witnesses). In the second case, the recipients (coordinators, AIPN, etc.) will have access to some data (not their own) because they need them to accomplish their task.

The **CEDEFOP** should therefore modify the *recipient* section of his privacy statement and the point 7.2 and 7.5 of his draft manual. The **ETF,** the **OHIM,** the **CDT**, the **EFSA,** the **EMCDDA** and the **FRONTEX** should also modify their documents accordingly (privacy statement, Declaration on the Protection of Personal Data, Opening form, Declaration of confidentiality regarding the informal procedure for cases of psychological or sexual harassment, etc.).

2.7. Rights of access and rectification

Article 13 of the Regulation provides for a right of access and sets out the modalities of its application following the request of the staff member concerned. Article 14 of the Regulation provides that *"the data subject shall have a right to obtain from the controller the rectification without delay of inaccurate or incomplete personal data"*.

Informal procedure

[4] See WP 29 document on the definition of consent adopted on 13 July 2011, 15-16.

[5] See also the Article 29 Working Party Opinion 8/2001on the processing of personal data in the employment context.

As quoted above, right of access and rectification are enforceable rights of the data subject. This reality should be reflected in the privacy statements of the **ETF**, the **CEDEFOP,** the **FRONTEX,** the **OHIM,** the **EMCDDA** and the **CDT** where Articles 13 and 14 are not at present properly quoted. Articles 13 and 14 are the general rule and any application of the limitations foreseen in Article 20 (1) (c) must be granted on a on a case by case analysis.
In the case of harassment, exemptions of Article 20 will most probably be used to defer the right of access of the alleged harasser to his/her own data. This limitation is applied to protect the alleged victim. The right of access of the alleged harasser is linked to the information he received on the procedure. An alleged harasser won't request access if he is not aware of an existing informal procedure involving him (see the point on information below).

The application of the limitations must be dealt with on a case by case basis by the controller (represented here by the confidential counsellors in most cases of soft data and the Coordinator/contact person in most cases of hard data) taking into considerations alleged victim's protection.

As to the description of the circumstances[6] where access will be granted, the EDPS recommends to the **CEDEFOP,** the **ETF,** the **CDT,** the **OHIM,** the **EMCDDA** and **FRONTEX** to either better emphasise that these circumstances are only examples or remove the examples that may lead to confusion and focus on legal substance.

The **ETF,** the **CDT,** the **OHIM,** the **EMCDDA and FRONTEX** should in any case distinguish access to documents and access to personal data, in particular in indent 4 which is not correct as such.

In his privacy statement on "(...) *sustaining a working culture based on dignity and respect*", the **EMCDDA** limits the right of access of the data subject in cases where data is inaccurate or incomplete. This limitation only applies to the right of rectification. The privacy statements should be adapted accordingly.

Selection of confidential counsellors

In the **EMCDDA** privacy statement, the right of rectification is limited after the closing date for submitting an application to data related to eligibility criteria. Contact details for instance could still be rectified. As for the access to their data, the limitations provided for in Article 20 may imply that access should be granted neither to the comparative data concerning other applicants (comparative results), nor to the individual opinions of the members of the selection committee if such access would undermine the rights of others applicants or the freedom of members of the selection Committee. Therefore, it should be clearly established that:

---

[6] Several agencies have included in their Manual or privacy statement the following text:

- *"All data subjects will be able to access the documents they have themselves transmitted;*
- *All data subjects, either alleged victim(s) or alleged mistreater(s), may have access to the opening sheet for the case relating to them. As far as alleged mistreaters are concerned, this access will only be granted if they have been informed by the confidential counsellor of the existence of an informal procedure, after the alleged victim has given his/her consent (with the exception already mentioned, i.e. need to protect the alleged victim);*
- *Alleged victims also have access to the closing form concerning their case;*
- *Access to any other document will only be granted if this document does not contain personal data relating to other persons or confidential statements, or if there is no risk that its transmission may impact negatively on one of the parties involved in the case, on the smooth running of the procedures or on future relations between the parties*.".

- the objective of any confidentiality requirement is to ensure that the selection committee is able to maintain its impartiality and independence and is not under undue influence from the controller, the candidates, or any other factor and
- any restriction on access rights must not exceed what is absolutely necessary to achieve this purported objective.

2.8 Blocking

With respect to the data subject's right to block data, the EDPS reminds the **CDT** that, in accordance with Article 15 of the Regulation, several situations must be distinguished:
(1) when the data subject contests the accuracy of his/her data, the data should be blocked "for a period enabling the controller to verify the accuracy, including the completeness of the data". Thus, when receiving a request for blocking on this ground, the **CDT** should immediately block the data for the period necessary for verifying the accuracy and completeness of the data;
(2) when the data subject requires the blocking of his/her data because the processing is unlawful, or when data must be blocked for purpose of proof, the **CDT** will need some time to make this assessment before deciding to block the data. In such cases, even though the request for blocking may not take place immediately, it should nevertheless be dealt with promptly in order to preserve the data subject's rights. Having considered this, the EDPS notes that the decision as to whether to block the data is taken by the **CDT** at the latest within the delay of 15 working days.

2.9. Information to be given to the data subject

Articles 11 and 12 of the Regulation provide that data subjects must be informed of the processing of data relating to them and list a range of general and additional items. The latter apply insofar as they are necessary in order to guarantee fair processing in respect of the data subject having regard to the specific circumstances of the processing operation. In the present case, the data processed in the framework of the selection of counsellors and the informal procedure are partly provided by the data subject and partly by various parties involved.

In the case of harassment, the information must be twofold: (i) the general information relating to the procedures put in place to fight against harassment (informal procedure, network of confidential counsellors) and (ii) the specific information to the data subjects directly involved in a particular procedure as alleged victim, alleged harasser, witness etc.

Informal procedure

General information: Privacy Statement

The **CEDEFOP,** the **ETF,** the **FRONTEX** and the **CDT** should modify their policy notice according to the points 2.7 and 2.8 of this Opinion. The **ETF** privacy statement should also mention the potential recipients of the data. The **OHIM** and the **Eurofound** did not provide the privacy statement mentioned in their notification. The EDPS must have a copy of the text to conduct his analysis. The **ECHA** privacy statement is very clear for the data subject.

Specific information

The **CDT** did not provide the EDPS with information concerning the specific information to be given to the data subject. The EDPS would like to receive clarification as to the implementation of this right.

The **EMCCDA** should add in the section "processed data" the notes of the confidential counsellors.

Selection of confidential counsellors

The **OHIM** mentions in his notification that data protection statements are available in the Charter of Ethics and in the **OHIM's** Guidelines. Both statements concern the informal procedure and not the selection of certified mediators of the **OHIM**. The **OHIM** also stated that the call of interest is sent to the data subject. The EDPS did not receive a copy of the data protection relevant part of the call of interest. The EDPS recommends **OHIM** to provide him with the relevant documents concerning the information to be given to the certified mediators of **OHIM**.

As for the selection of confidential counsellor by the staff committee, the **OHIM** should modify his Data Protection Statement according to Articles 11 and 12 of the Regulation. The recipients of the data, the legal basis and the time limit for storing the data should be added. The main ground to make the processing legitimate is to be found in Article 5 (a) -the legitimate performance carried out in the public interest- and the consent of the data subject. This should be modified accordingly.

The EDPS did not receive the Data Protection Policy statement included on the Intranet site and on the application form from the **EUROFOUND**. The EDPS should receive a copy of the text to conduct his analysis.

2.10. Security

According to Article 22 of the Regulation, *"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".*

The **EUROFOUND** set up a Declaration of confidentiality to be signed by each confidential counsellor. A reference is made to the fact that they should only process the data for the purpose for which they where transmitted. This principle is laid down in Article 7 and not in Articles 11 and 12. The Declaration should be modified accordingly.

2.11. Processing data on behalf of controllers

Article 2 (e) of the Regulation states that *"'processor' shall mean any natural or legal person, public authority, agency or any other body which process personal data on behalf of the controller".* Article 23 of the Regulation stipulates on one hand, the role of the processor and on the other hand, the obligations of the controller in ensuring sufficient guarantees in respect of the technical and organisational security measures and ensuring compliance with those measures.

In the **ETF** privacy statement, the confidential counsellors and the contact person are considered as "processors". The **EMCDDA** also prepare a Data Protection declaration for confidential counsellors where they are considered as "processor". The EDPS is not in favour of the distinction controller/processor within an Agency[7]. The EDPS encourages an approach

[7] The EDPS recommends in his Article 28.1 consultations relating to the implementing rules concerning the tasks, duties and powers of the Data Protection Officer not to use the notion of processor within an Agency. See among other the consultation on the implementing rules pursuant to Article 24.8 adopted by the European

of co-responsibility between the administration department (including the contact person) and the confidential counsellors. The privacy statement and the Data Protection Declaration must be adopted accordingly, bearing in mind that the Agency itself, as the controller of the processing operations, is responsible for implementing appropriate technical and organisational measures a level of security appropriate to the risks represented by the processing in accordance to Article 22.

As **ECHA** is aware[8] of, the reference to the rights of the data subject (access, rectification, recourse to the EDPS) mentions the contractor as the beneficiary of these rights, whereas according to the data protection regulation any person concerned by the processing of the data by processor should be entitled to exercise his/her rights. The contract should further specify that the processor should only process personal data on instructions of **ECHA**. The EDPS therefore invites the **ECHA** to revise the present clause.

Conclusion

The EDPS Guidelines have been a useful tool for agencies to reflect on how the data protection principles of the Regulation have an impact on the processing of data in the framework of harassment and set up their own procedures.

The next step forward is that all the specific recommendations highlighted by the EDPS in the present Opinion are fully implemented by each of the nine agencies concerned. In light of the EDPS' recent policy paper on monitoring and ensuring compliance with the Regulation[9], the controller of each agency concerned is now invited to adopt specific and concrete measures, namely revise its draft rules, adopt documents, modify or add provisions and principles etc. as underlined by the EDPS in this Opinion. Other recommendations request agencies to provide further information about their procedure. Each agency should therefore provide the EDPS with all relevant documents within three months of issuing the Joint Opinion.

Done at Brussels, 21 October 2011

(**signed**)

Giovanni BUTTARELLI
Assistant European Data Protection Supervisor

Research Council Executive Agency. This is supported by Article 1(1) of the Regulation which appoints institutions and bodies as the only actors who "shall protect" the right to privacy of the data subject and who "shall neither restrict nor prohibit" the free flow of personal data. See Also WP29 Opinion 1/2010 on the notion of controller.

8 See Opinion 2010-109 on recruitment.

9 Monitoring and Ensuring Compliance with Regulation (EC) 45/2001 Policy paper, Brussels, 13 December 2010