

Opinion on a notification for Prior Checking received from the Data Protection Officer of the Office for the Harmonization in the Internal Market (OHIM) regarding the selection of managers

Brussels, 12 November 2008 (Case 2008-435)

1. Proceedings

On 11 July 2008, the European Data Protection Supervisor (**EDPS**) received from the Data Protection Officer of the Office for Harmonization in the Internal Market (**OHIM**) a Notification for prior checking concerning the data processing operations that take place in the context of the selection of managers in OHIM (**Notification**).

On 8 October 2008 the EDPS sent the draft opinion to the Data Protection Officer for comments which were received on 10 November 2008.

2. Examination of the matter

OHIM organises and manages the selection process of managers in order to select the best suited candidates for a particular position. The positions are open to internal candidates and in some cases vacancies are also open to external candidates.

Prior to starting the selection, OHIM publishes vacancy notices of the available posts. The publication is always on-line, on OHIM's Website. OHIM's Appointing Authority (**AA**) designates a **Selection Committee** responsible for the procedure.

2.1 The Facts

The *purpose* of the data processing operations is to manage the selection of managers in order to select the best suited candidates for each particular position.

The *primary responsibility* for the data processing lies within the Human Resources Department of OHIM. The data processing operations are carried out by the Selection Committee, by its Secretariat and by the Internal Mobility and Recruitment of Managers Section of the Human Resources Department (**IMRMHRD**).

The data processing operations that take place in the selection of managers in OHIM are both manual and electronic and can be summarised as follows:

- i The applicant files his/her application electronically via the OHIM e-recruitment webpage at: https://service.oami.europa.eu/erecruitment/la/en_form.cfm or through the e-mail address indicated in the vacancy notice. The application will include (a) a motivation letter,

if relevant; (b) the curriculum vitae (**CV**) drafted by the applicant (normally the EU standard Europass CV); (c) an indication of the language skills; (d) an indication of any other competencies and knowledge areas that the applicant may find relevant to the vacancy as published. Whenever the applicant is an internal member of staff, he/she will describe his skills as collected in the most recently available annual appraisal report.

- ii The Selection Committee examines the admissibility of the applications received and establishes a list of the admissible applicants.
- iii The admissible applicants may be asked to undergo tests through an external consultant who will submit the results to the Selection Committee.
- iv On the basis of the applications, the CV and the results of the tests, the Selection Committee will invite the most suitable candidates for an interview according to the criteria announced in the vacancy notice as published.
- v After the interviews, the Selection Committee assesses the profiles of the candidates and draws up a list or a reserve list of candidates and a final explanatory report. The reserve list is signed by the AA and published.
- vi The candidates are informed by letter of the outcome of their application.

The *types of data subjects* whose data are collected in the course of the selection of candidates for management posts within OHIM include the following: (i) officials of the EU institutions and, (ii) external applicants, i.e. individuals who are not permanent officials, civil servants of the EU institutions and who apply for a given position (altogether **candidates**).

The *categories of data* collected and further processed include the following: (i) identification data, which may include surname, first name, date (and place) of birth, sex, nationality, telephone number, email address; (ii) education and professional experience, which may include the degree/diploma, date of award of degree, length of professional experience, length of management experience, languages spoken and level, previous working experience in the European Institutions and personnel number (if applicable); (iii) data related to the suitability of a candidate for a particular vacancy which includes (a) the assessment made by the Selection Committee when it matches the applications received with the selection criteria; (b) the performance of candidates during the assessment tests as recorded by the human resources consultant and, (c) the performance of candidates during the interviews. Finally, it also includes the list of successful and non-successful candidates and related final explanatory report.

As far as the *conservation* of the data is concerned, all the information is stored on-line in the directory for Personnel/Career and Development Sector. This information is only accessible by the members of the IMRMHRD and by member of the Selection Committee.

According to the Notification, the selection dossiers, including the summaries of the tests, are destroyed 5 years after the end of the selection procedure and publication of the final list of successful candidates. For successful candidates, their data are stored for an unlimited period of time as it will remain in the personal folder of the individual.

The relevant paper documents are stored in the folders specific to each selection procedure in the premises of the **IMRMHRD**.

The data controller may *transfer personal data* gathered in the context of the selection of managers in OHIM to the following types of recipients: (i) Whenever relevant, the selection files necessary for the consultant to carry out its job will be transmitted to the external consultant. In this case, a contract will be signed with the consultant that will include a clause stating that the consultant must comply with the requirements of Regulation (EC) No 45/2001. (ii) Candidates' related information (list and related report) is sent to the AA.

As far as the *right to information* is concerned, the Notification explains that information to candidates is given either by email or through the e-recruitment website. This takes place when candidates register on-line for a particular vacancy. A copy of the privacy statement was annexed to the Notification. A member of the EDPS staff visited the e-recruitment web site to check how the information was provided to candidates. In contrast to what was stated in the Notification, no privacy statement is placed on the e-recruitment website of OHIM, where candidates have to register their information (https://service.oami.europa.eu/erecruitment/la/en_form.cfm). However, there was a privacy statement in the "career opportunities Web site" but its content was not the same as the one provided to the EDPS. It is uncertain how the two privacy statements fit together.

The privacy statement provided to the EDPS contains information on the identity of the data controller, legal basis, the existence of a right of access and the right to rectify. The privacy statement does not contain any reference to the external consultant.

As far as *access rights and rectification* are concerned, as described in the privacy statement, individuals are recognised such rights and they are informed that they can be exercised by contacting the data controller. No email for the exercise of these rights is provided and no further information is given about the procedure.

As far as *security measures* are concerned, the data controller acknowledges that it has put technical measures in place to ensure the level of security appropriate to the risks, and to prevent any unauthorised disclosure or access, accidental or unlawful destruction or accidental loss or alteration, and to prevent all other unlawful forms of processing. (...)

2.2. Legal Aspects

2.2.1. Prior Checking

This Notification relates to the procedure that takes place within the Human Resources Department of OHIM towards hiring managers. It starts with the publication of a vacancy and ends when the most suitable candidate is selected. This Opinion will not address data processing operations that go beyond this scope. For example, the data processing that takes place after the selected candidate has accepted the job.

Applicability of the Regulation. Regulation (EC) No 45/2001 applies to the "processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system" and to the processing "by all Community institutions and bodies insofar as such processing is carried out in the exercise of activities all or part of which fall within the scope of Community law"¹. For the reasons described below, all elements that trigger the application of the Regulation are present here:

¹ See Article 3(2) of Regulation (EC) No 45/2001.

First, the selection of managers at OHIM entails the collection and further processing of *personal data* as defined under Article 2(a) of Regulation (EC) No 45/2001. Indeed, as described in the Notification, personal data of individuals who apply for management positions in OHIM are collected and further processed.

Second, as described in the Notification, the personal data collected undergo "*automatic processing*" operations, as defined under Article 2(b) of the Regulation (EC) No 45/2001 as well as manual data processing operations. Indeed, some of the personal information is collected electronically directly from applicants. Other information is created by the Selection Committee on the basis of the candidates' performance and is stored electronically.

Finally, the processing is carried out by a Community body, in this case OHIM, in the framework of Community law (Article 3(1) of the Regulation (EC) No 45/2001). Therefore, all the elements that trigger the application of the Regulation are present.

Grounds for Prior Checking. Article 27(1) of Regulation (EC) No 45/2001 subjects to prior checking by the EDPS "*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. This list includes, under paragraph (b), the processing operations intended to evaluate personal aspects related to the data subject, including his or her ability, efficiency and conduct. The processing operations that occur in the context of selecting managers in OHIM precisely aim at evaluating the capacity of each candidate for a particular position. In order to carry out such an evaluation, the data controller will perform various assessment activities such as weighing up whether the individual in question matches the selection criteria, judging his/her performance during the interviews, judging the performance of each candidate in his/her current positions, etc. In sum, taking the above into account, clearly the data processing operations fall within Article 27(2) (b) and must therefore be prior checked by the EDPS.

Ex-post Prior Checking. 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 operations have already been established. This is not an insurmountable problem provided that all recommendations made by the EDPS are fully taken into account and the processing operations are adjusted accordingly.

Notification and Due Date for the EDPS Opinion. The Notification was received on 11 July 2008. The period within which the EDPS must deliver an opinion was suspended for a total of 33 days to allow for comments on the draft EDPS Opinion. In addition, the two months period deadline was also suspended during the month of August. The Opinion must therefore be adopted no later than 13 October 2008.

2.2.2. Lawfulness of the Processing

Personal data may only be processed if legal grounds can be found in Article 5 of Regulation (EC) No 45/2001. As pointed out in the Notification, the grounds that justify the processing operation are based on 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*".

In order to determine whether the processing operations comply with Article 5(a) of Regulation (EC) No 45/2001, two elements must be taken into account: First, whether either the Treaty or other legal instruments foresee a public interest task, and second, whether the processing operations carried out by the data controller are indeed necessary for the performance of that task.

Legal Basis. In ascertaining the legal grounds in the Treaty or in other legal instruments that legitimise the processing operations that take place in the context of the selection of managers in OHIM, the EDPS takes note of the following legal instruments: (i) Article 29 of the Staff Regulations which establishes the criteria for filling vacant posts in institutions. In particular, it refers to competition procedures (Art. 29.1) and to other types of procedures (Art. 29.2) "*for the recruitment of senior officialsand, in exceptional cases, also for recruitment to posts which require special qualifications*". (ii) Article 12 of the Conditions of Employment of other Servants foresees the creation of procedures and selection criteria of temporary staff. Thus, both Art 29 of the Staff Regulation and Art 12 of the Conditions of Employment of other Servants authorise the European institutions, in this case OHIM, to engage in selection procedures to recruit officials or other servants for management positions. In conclusion, the EDPS considers that the data processing that occurs in the context of the selection of managers is legally based on the above legal instruments.

Necessity Test. According to Article 5(a) of Regulation (EC) No 45/2001, the data processing must be "*necessary for performance of a task*" as referred to above. It is therefore relevant to assess whether the data processing that occurs in the context of the selection of managers is "*necessary*" for the performance of a task, in this case, for the selection of the best suited candidates.

As outlined above, under the Staff Regulations and Conditions of Employment of other Servants OHIM is entitled to adopt procedures to recruit candidates for management positions. To put into practice this provision, it is necessary for OHIM to collect and further process personal information of candidates. Unless OHIM collects CVs and motivation letters and unless it can test the candidates through various procedures in order to evaluate their competences and whether they match the selection criteria, it would not be possible for OHIM to ensure a fair selection of candidates. In conclusion, it is the EDPS's view that the data processing that takes place in the context of the selection of managers is necessary to ensure the selection of the best candidates in an open, fair and transparent way.

2.2.3. Processing of Special Categories of Data

Article 10.1 of Regulation 45/2001 establishes that "*the 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*". The prohibition is lifted if grounds can be found in Articles 10(2) and 10(3) of the Regulation. Among others, such grounds include the consent of the data subject ex Article 10(2)(a).

The Notification states that no data falling under the categories of data referred to in Article 10.1 are processed in the context of the data processing operations notified for prior checking. Taking into account the overall purpose pursued by OHIM when it engages in data processing operations to select managers, the EDPS understands that the collection of special categories of data is not OHIM'S intention in the context of such a selection. Indeed, the gathering of special categories of data does not seem very helpful towards selecting candidates insofar as such data may be irrelevant for the purposes of selecting the best suited candidate. However, the EDPS considers that in the context of selecting candidates for management positions,

applicants may reveal information about their disability or other types of special categories of data. For example, if they send pictures revealing their racial or ethnic origin. If this occurs, it should be considered that candidates have given their consent to the processing of that data, thus, the condition of Article 10(2) (a) would be met. In addition, if the data are relevant, this consent is given in the context of staff management (recruitment) in order to enable the employer to comply with his specific obligations in the field of employment law, for example to provide for extra time and to provide specific IT equipment for the tests, ex Article 10(2)(b) of the Regulation according to which the prohibition shall not apply where the processing is "*necessary for the purpose of complying with the specific rights and obligations of the controller in the field of employment law insofar as it is authorised by the treaties establishing the European Communities or other legal instruments adopted on the basis thereof*".

Article 10.5 of Regulation (EC) No 45/2001 establishes that "*[processing of data relating to offences, criminal convictions or security measures may be carried out only if authorised by the Treaties establishing the European Communities or other legal instruments adopted on the basis thereof or, if necessary, by the European Data Protection Supervisor.*" According to the Notification no such data are collected in the context of the selection of candidates for management positions.

2.2.4. Data Quality

Adequacy, Relevance and Proportionality. Pursuant to Article 4(1)(c) of Regulation (EC) No 45/2001, personal data must be adequate, relevant and non excessive in relation to the purposes for which collected and/or further processed. This is referred to as the data quality principle.

The type of information requested to apply for a management position includes a motivation letter and CV, language skills and indication of any other competencies and knowledge areas that the candidate may find relevant to the vacancy. The EDPS considers that this information is adequate and relevant in relation to the purposes for which they are intended to be used (to determine whether a candidate complies with the minimum conditions of eligibility for a management position) and thus complies with Article 4(1)(c) of Regulation (EC) No 45/2001.

Fairness and Lawfulness. Article 4(1)(a) of the Regulation requires that data must be processed fairly and lawfully. The issue of lawfulness was analysed above (see Section 2.2.2). The issue of fairness is closely related to what information is provided to data subjects which is further addressed in Section 2.2.8.

Accuracy. According to Article 4(1)(c) of the Regulation, personal data must be "*accurate and, where necessary, kept up to date, and every reasonable step must be taken to ensure that the 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*". In this case, an important part of the data has been provided by the applicant himself/herself. This procedure itself helps to guarantee the accuracy of the personal data. However, other information is not provided directly by the individual but generated by the various Selection Committee and external consultant. In this regard, as further developed below, it is important for the candidate to be able to exercise the right of access and rectification insofar as it enables him/her to control whether the data hold about him/her is accurate. In this respect, see also Section 2.2.7.

2.2.5. Conservation of Data

Pursuant to Article 4(1)(e) of Regulation (EC) No 45/2001 personal data may be kept in a form which permits identification of data subjects for no longer than necessary for the purposes for which the data are collected and/or further processed.

According to the Notification, the selection dossiers, including the summaries of the tests, are destroyed 5 years after the end of the selection procedure and publication of the final list of successful candidates. The EDPS considers that the period of 5 years is appropriate for purposes of facing possible challenges for non-selected candidates; this is also the approximate period during which documents are required to be kept under the Financial Regulation.

The EDPS also considers it appropriate to keep data of successful candidates for a longer period insofar as such data will have to be processed in the context of their employment relationship with OHIM. This Opinion does not address the adequacy of such retention periods, which need to be reviewed in the context of each particular data processing operation.

2.2.6. Transfers of Data, including to Processors

Articles 7, 8 and 9 of Regulation (EC) No 45/2001 set forth certain obligations that apply when data controllers transfer personal data to third parties. The rules differ depending on whether the transfer is made to (i) Community institutions or bodies (based on Article 7), (ii) to recipients subject to Directive 95/46 (based on Article 8), or (iii) to other types of recipients (based on Article 9).

According to the Notification, the data controller may *transfer personal data* gathered in the context of the selection of managers in OHIM to the following types of recipients: (i) The reserve list of successful candidates and related report is sent to the AA for final decision and signature; (ii) whenever relevant, the selection files necessary for the external consultant to carry out his job will be transmitted to the external consultant.

The transfer described under (i) is made within a Community body and it is thus governed by Article 7 of Regulation (EC) No 45/2001 which requires personal data to be transferred "*for the legitimate performance of tasks covered by the competence of the recipient*". The EDPS considers that the transfer to the AA complies with this requirement insofar as the AA has the competence to make the final selection.

The transfer described under (ii) is made to an external consultant (contractor) which is subject to Directive 95/46². The contractor is bound by national data protection legislation implementing Directive 95/46. The EDPS considers that the contractor is a data processor as defined under Article 2 (e) of Regulation (EC) No 45/2001. The Notification confirmed that a confidentiality agreement is signed every time that the contractor services are used which, among others, imposes upon the contractor the obligation to adopt appropriate technical and organisational security measures to protect the personal data. Please note that the applicable security measures are those to which the data processor is subject *ex application* of the national law that implements Directive 95/46. For example, if the data processor is established in Spain, it will be subject to the technical and organisational security measures

² Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

required under the Spanish data protection legislation. This should be reflected in the agreement.

2.2.7. Right of Access and Rectification

According to Article 13 of Regulation (EC) No 45/2001, the data subject shall have the right to obtain without constraint from the controller, communication in an intelligible form of the data undergoing the processing and any available information as to their source. Article 14 of the Regulation provides the data subject with the right to rectify inaccurate or incomplete data.

According to the privacy statement and Notification, candidates are recognised such rights and they are informed that they can be exercised by contacting the data controller. However, no email for the exercise of these rights is provided and no further information is given about the procedure.

The applicant's right of access enables them to see that the Selection Committee has acted fairly and objectively. Such a right does not interfere in any way with the principle of equal treatment of applicants since it is open to all of them. Given the importance of this right, the EDPS recommends that OHIM sets up procedures to ensure access to candidates' personal data as described below. Furthermore, the EDPS recommends that OHIM provides to candidates information about the procedures to exercise the right of access, in the privacy statement.

Regarding the procedures to provide the rights of access and rectification and the scope of such rights, the following should be taken into account:

(i) OHIM must ensure that individuals have the right to access not only the information that they submitted but also their entire file, comprising the results of the tests and notes concerning them drafted by the Selection Committee and by the external consultant. To this end, it would be appropriate for the privacy statement to describe such rights and to provide an email address to this effect.

The EDPS is aware that there is a limitation to the right of access in this context. Indeed, the principle of the secrecy of Selection Committee's proceedings, as set out in Article 6 of Annex III of the Staff Regulations, allows for the limitation on the right of access. The limitation to the right of access can also be invoked on the basis of in Article 20(1)(c) which foresees the restriction of such rights as a measure necessary to safeguard the protection of the data subject or of the rights and freedoms of others. This means that no marks given by individual members of the committee should be given. Furthermore, information comparing the data subject with other applicants should not be provided. The EDPS calls upon OHIM to ensure the application of the right of access as described above.

(ii) The right of rectification can obviously apply only to factual data. Marks allocated could not under any circumstances be open to a right of rectification by the data subject, except in the context of the established appeals procedures. Furthermore, the EDPS notes that limitations to the right of rectification of candidates' data, after the deadline for the sending of documents regarding a given competition may be necessary for different reasons, including of practical nature. In this regard, the EDPS considers these limitations can be seen as necessary to ensure objective, certain and stable conditions for the competition, and essential to the

fairness of processing. Thus it can be recognised as a necessary measure under Article 20(1)(c) of the Regulation for the protection of the rights and freedoms of others.

2.2.8. Information to the Data Subject

Pursuant to Articles 11 and 12 of Regulation (EC) No 45/2001, 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.

In order to comply with this obligation, according to the Notification information is given to candidates either by email or through the e-recruitment website. This takes place when candidates register on-line for a particular vacancy. A copy of the privacy statement was annexed to the Notification.

As stated under section 2.1., the EDPS checked how information was provided to candidates on the e-recruitment web site and found that this web site had no specific privacy statement (other than the one of a more general nature in the "career opportunities Web site").

The EDPS recommends that the privacy statement is provided on the web page where individuals have to register their information. It must be placed in a visible way, for example, it could be provided through a pop-up window interactively on the screen. Alternatively, it could be provided through a link requiring individuals to click a box pursuant to which individuals would state that they have read the privacy statement. Furthermore, it should be placed in a way that permits it to be printed and saved.

Regarding the content of the information provided in the privacy statement, the EDPS considers that it should be complemented in order to ensure compliance with Articles 11 and 12, in particular:

- (i) In order to ensure full transparency and fair processing, it would be appropriate to provide more information about the processing operations, including a reference to the various actors involved (such as the external consultant) in the processing operations.
- (ii) The procedures for the exercise of the right of access should be described, including the right of access regarding information held by the consultant. An email or contact point for the exercise of the right of access should be provided
- (iii) The time limits for storing the data should be included.

2.2.9. Security measures

According to Articles 22 and 23 of Regulation (EC) No 45/2001, the controller and the processor must implement the 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. These security measures must in particular prevent any unauthorised disclosure or access, accidental or unlawful destruction or accidental loss, or alteration and prevent all other forms of unlawful processing. OHIM acknowledges that it has adopted the security measures required under Article 22 of the Regulation.

Independently of the above, taking into account the sensitivity of the personal data processed, the EDPS considers that it would be useful to raise awareness among personnel of OHIM and

in particular for those working in the secretariat of the Selection Committee and in the IMRMHRD. This should include training and signing a specific confidentiality declaration.

3. Conclusion

There is no reason to believe that there is a breach of the provisions of Regulation 45/2001 providing the considerations in this Opinion are fully taken into account. In particular, OHIM must:

- Set up a procedure for providing access rights. In particular, ensure that candidates have access to their file comprising assessment notes concerning them drafted by the Selection Committee and the external consultant. This applies without prejudice to the application of Article 20(1) (c) of Regulation 45 /2001;
- Provide to candidates information about the procedures to exercise the right of access, including an email address;
- Update the processor contract to reflect the application of national law to the security measures that must be implemented by processors;
- Amend the privacy policy as recommended in this Opinion and upload it in a visible place on web site;
- Raise awareness among OHIM (staff working for secretariat of the Selection Committee and those in charge of internal mobility and recruitment of managers within the Human Resources Department) regarding the need to ensure the confidentiality of the information. This should include training and signing of a specific confidentiality declaration.

Done at Brussels, 12 November 2008

(Signed)

Joaquín BAYO DELGADO
Assistant European Data Protection Supervisor