Opinion on the notification for prior checking received from the Data Protection Officer ("DPO") of the Office for Harmonization in the Internal Market ("OHIM") regarding the granting of "Social Financial Aid"

Brussels, 3 July 2007 (Case 2007-172)

1. Proceedings

On 16 March 2007, OHIM's DPO informed the European Data Protection Supervisor ("**EDPS**") via e-mail about OHIM's data processing operations related to its granting of "Social Financial Aid". On 23 March 2007, the EDPS received the formal prior checking notification ("**Notification**") by regular mail.

On 5 April 2007 the EDPS requested further information from OHIM. OHIM's DPO replied on 18 April 2007. On 28 May the EDPS requested additional information. OHIM responded on 18 June 2007. The procedure was further suspended for 4 days between 25 June and 29 June 2007, which was used by OHIM to comment on the draft EDPS Opinion. Finally, the procedure was extended by one week due to the complexity of the matter in accordance with Article 27(4) of Regulation (EC) 45/2001 ("**Regulation**").

2. Examination of the matter

2.1. The facts

2.1.1. Introduction. The notified processing operations consist of OHIM's granting of social financial aid to its employees. The processing operations are based on Article 76 of the Staff Regulations of Officials of the European Communities ("**Staff Regulations**") and the Conditions of Employment of other servants of the European Communities ("**Conditions of Employment**")[1]. This Article provides the following: "Gifts, loans or advances may be made to officials, former officials or where an official has died, to those entitled under him who are in a particularly difficult position as a result inter alia of serious or protracted illness or by reason of a disability or family circumstances."

The processing operations are primarily carried out by the social worker in OHIM's human resources department, but others, including the finance department, OHIM's medical officer, and outside medical experts may also be involved at certain stages of the processing.

[1] For the sake of brevity, these two documents together will sometimes be referred below as "**Staff Regulations**".

OHIM grants two types of social financial aids: (i) salary advance payment to staff members in particularly difficult circumstances, and (ii) aid to OHIM staff members to help finance non-medical expenses arising from disability.

2.1.2. Salary advance. The social worker's internal note of 6 June 2002 briefly describes the procedure and criteria for granting a salary advance.

According to the note, salary advance is granted only as an exceptional measure and only to staff members in particularly difficult circumstances. The salary advance may only be granted if other sources such as bank loans or financial assistance from family members are not available. When granting a salary advance, the social worker must take into account all relevant health, social and family circumstances of the staff member.

The social worker assesses the case based on her discussions with the applicant and the documents submitted by the applicant. The information requested to be provided and the level of detail depends on the circumstances of the case. The documents requested may include, among others, and in addition to the application form, a certificate indicating the amount of the applicant's salary, documents supporting the financial difficulties of the applicant (judgments, bank extracts, invoices, etc), and an excel file with a breakdown of the applicant's income and expenditures.

Only the social worker has access to the documents and information provided, and the information is used for the sole purpose of assessing the applicant's eligibility for salary advance.

The social worker’s assessment may be positive or negative, and may include a reservation. This assessment is written and communicated to the applicant. If the assessment is positive, the authorizing officer (currently the director of OHIM's Human Resources Department) is requested to confirm the availability of funds. If the availability of funds is confirmed, the social worker transfers the application form to the finance department. The finance department thereafter processes the payment.

The application form itself does not contain the reasons why the salary advance was granted. Instead, it only states that the applicant “requests a salary advance of EUR ... for the reasons discussed with the Social Administration Sector”. The application also specifies the bank account where the salary advance is to be paid and states that the salary advance is to be repaid by “... monthly deductions of EUR... from salary, starting in (month) ...”.

There are no further rules, for example, specifying how much advance can be granted and for how long.

2.1.3. Financial aid for disability. As noted in Section 2.1.1 above, both types of social financial aid are based on Article 76 of the Staff Regulations. In addition, to establish the detailed conditions for granting financial aid for disability, OHIM also adopted a specific decision. Decision no ADM 05-38 regarding complementary aid for the disabled ("**OHIM Decision**") sets forth the eligibility criteria and the procedure to grant complementary aid for the disabled, that is to say, aid to cover non-medical expenses related to disability.

The reimbursement may cover items such as costs of residence in an institution or home for the disabled, costs of education or training, costs of care by a qualified home nurse, and certain transportation expenses. The cost of certain appliances may also be partially

reimbursed. Reimbursement is made on a sliding scale, proportionate to the combined family income of the staff member.

According to the OHIM Decision, the persons eligible for the aid include officials and temporary staff in active employment, as well as their dependent spouses and children if they are at least 30% physically or 20% mentally disabled.

Procedures according to the OHIM Decision. The decision to grant support under the budget heading "complementary aid for disabled" is taken by the "Authority designated for that purpose".

The application for recognition of disability must include a detailed assessment of the measures necessary to offset the effects of disability and facilitate social integration. It must be accompanied by a medical report by the person's doctor, under sealed cover.

After receipt of the application, the Authority forwards the report to the medical officer of OHIM for an opinion. The medical officer, if necessary, may examine the disabled person. Based on the medical opinion and the eventual examination, the medical officer determines whether the 30% or 20% threshold is met, and issues a medical opinion on that matter.

Before taking its decision, the Authority may seek the opinion of an *ad hoc* committee consisting of OHIM's medical officer, the social worker, the administrator responsible for the case concerned, and, if necessary, two experts appointed by the President of OHIM. The committee assesses the social integration problems resulting from the disability and delivers an opinion on the measures advocated to offset such effects.

The Authority takes its decision based on the opinion of the medical officer, and, when consulted, based on the opinion of the *ad hoc* committee. The decision specifies the services covered by the financial support granted by OHIM. The decision is then notified to the person concerned.

Once approved, bills for reimbursement are sent to the settlements office of the Joint Sickness Insurance Scheme ("**JSIS**") or directly to the welfare unit of OHIM, depending on whether the bills included expenses reimbursable under the JSIS. Whenever possible, bills must be itemized. Reimbursement is granted after the recipient has claimed all possible national aid, which is taken into account when calculating the amount of the financial support. The recipient must also provide documentary evidence of dealings with, and aid paid by, national administrations.

Implementation of the OHIM Decision: the processing in practice. As a practical matter, applicants submit their applications to the social worker who is the first to review the application, except for the medical documents, which she receives in a sealed envelope.

The social worker forwards the medical documents in the same sealed envelope as received to the medical officer for an opinion. She has no access to the content of the envelope.

Although a possibility is provided under the OHIM Decision, in practice, the medical officer does not physically examine the disabled persons but carries out his or her assessment based on the documents alone. The medical opinion of the medical officer includes the final conclusion "staff member meets the condition under Article 4(1) of Decision no ADM 05-38" and does not include additional medical data. The medical officer sends his or her opinion to the social worker.

The "Authority" referred to in the OHIM Decision is the so-called "authorizing officer". As OHIM explained to the EDPS, the role of the authorizing officer, as a matter of fact, is limited to budgetary implications, that is to say, he or she is there to make sure funds are or may be made available under the appropriate budget line. According to the current organizational structure, the authorizing officer is the head of OHIM's Human Resources Department.

In practice, it is always the *ad hoc* committee comprising of the social worker, the authorizing officer and the medical officer who jointly carries out the assessment and adopts the decision regarding the acceptance of the application based on the social and medical circumstances of the case. In some cases, as necessary, two outside experts are also designated.

The decision of the *ad hoc* committee takes form of a "note to file". The note to file and any other "adversely affecting decisions" in the process are subject to appeal under Article 90 of the Staff Regulations.

OHIM submitted to the EDPS, along with its Notification, a sample note to file. The text did not detail the medical condition of the disabled person or the social, personal, and family circumstances of the applicant. Nevertheless, the note to file contained certain sensitive personal data: in particular, it designated the percentage of disability. In addition, in the sample provided, the measure consisted of special needs education for the staff member's dependent child. In this case, the name of the educational institute itself could indirectly suggest the nature of the disability. There may be other incidental facts related to other measures that may similarly disclose certain information regarding the disability. The decision may mention, for example, the type of equipment that is to be co-financed with the applicant.

As for financial information, the sample note to file specified a percentage figure as being the official's own contribution to the costs incurred. The note to file, however, did not reveal further financial details such as the actual cost of the financing. With that said, the authorizing officer is one of the members of the *ad hoc* committee. His or her role, as noted above, is to make sure that the estimated costs can be supported by the appropriate budget line. Cost estimates, at this stage, are calculated based on invoices or cost estimates provided by the applicant.

Following the adoption of the note to file, the authorizing officer also draws up a separate document summarizing the financial implications of the note to file in an Excel table. This document includes the actual costs, as well as percentages of reimbursement. The document also contains a brief description of the measures to be financed.

The social worker circulates the note to file and the Excel table to the financial department in order to implement the financial aid in accordance with the requirements of OHIM's Financial Regulation (commitment and payment). The supporting documents are not transferred to the financial department.

2.1.4. Recipients of the data. OHIM explained that the medical documents used during the evaluation of applications are kept with the medical officer under lock and key. These documents may include, for example, personal notes or analysis of the medical officer and the opinion of the applicant's doctor on the nature and extent of the disability. No one other than the medical officer has access to these documents.

As for all other documents submitted by the applicant to support his/her application and which may contain health-related, social, financial or other personal data, only the social worker have access to them. They are held under lock and key by the social worker. When the *ad hoc* committee is convened, it also has access to the same documents. The documents held by the social worker may include, for example, a disability certificate stating the degree of disability, proof of income of spouses and allowance received for the dependent child, proof of educational allowance, detailed programme for the activity planned, and invoices.

The finance department does not have access to any of the supporting documents included in the applications. It does, however, receive the note to file prepared by the *ad hoc* committee, the Excel table drawn up by the authorizing officer, and the application for salary advance. These documents, as described above, only contain personal data on a need-to-know basis. No other documents are foreseen to be submitted to the finance department.

At the time when it comes to actual payment of the aid, the applicant must submit detailed invoices evidencing that the amounts were actually incurred. These are kept by the social worker. Finally, as described above, bills for reimbursement may also be sent to the settlements office of the JSIS.

Other than those mentioned here, no data transfer is foreseen to either third parties or others within OHIM.

2.1.5. Information provided to data subjects. The application for salary advance provides a data protection notice. This notice specifies the purpose of the processing, recipients, and conservation period, as well as rights of access. No such information is currently provided with respect to the disability aid, but during the prior checking procedure, OHIM proposed that in the future it could include the necessary information (i) in all email exchanges with applicants, (ii) on the intranet, and that (iii) the OHIM Decision could also be modified to include a specific provision on data protection.

2.1.6. Access rights. OHIM explained that data subjects can exercise their rights of access by sending a written request to the social worker.

2.1.7. Conservation period. Article 38(6) of OHIM's Financial Regulation provides the following: "the authorising officer shall conserve the supporting documents relating to operations carried out for a period of five years from the date of the decision granting discharge in respect of implementation of the budget." Pursuant to this provision, as a matter of fact, the files at OHIM are kept for a period up to between six and seven years, considering that the decision granting discharge occurs during the year after the one in which an operation was carried out and the five-year period only starts to run as of the date of the discharge. No data is stored for historical, statistical or scientific purposes.

2.1.8. Security. Access to all OHIM computers that may contain data related to any of the processing operations described in this Notification are password-protected. All documents are stored in locked cupboards, with keys available on a need-to-know basis only. All documents related to granting the aid are marked "confidential", generally in their respective headers and on routing sheets.

2.2. Legal aspects

2.2.1. Prior checking

Applicability of the Regulation. Pursuant to its Article 3(2), the Regulation applies to the processing of personal data by 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. Personal data is defined as any information relating to an identified or identifiable natural person. Article 3(2) further provides that the Regulation applies to the processing of personal data wholly or partly by automatic means, as well as to non-automatic processing of personal data which form part of a filing system or are intended to form part of a filing system.

OHIM is a Community body, and the granting of social financial aid forms part of the management of its own internal activities, and therefore, it is within the scope of Community law. There is also no doubt that the processing involves personal data. The documents are organized into filing systems. The Regulation, therefore, applies.

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

This list specifically includes, under paragraph (b), processing operations intended to evaluate personal aspects relating to the data subject, including his or her ability, efficiency, or conduct. The notified processing operation involves processing operations intended to evaluate personal aspects relating to the data subject, in particular, his or her financial, social, and family circumstances, and his or her eligibility for the aid based on a pre-set criteria.

In addition, the Article 27(2) list also specifically includes, under paragraph (a), processing of data relating to health. In case of the disability aid the processing always involve health-related data. In case of salary advances the processing may, at least some of the times, involve health-related data.

Based on the foregoing, the processing requires prior checking by the EDPS.

Timing of the Notification and due date for the EDPS Opinion. The Notification was received on 23 March 2007. According to Article 27(4) of the Regulation this Opinion must be delivered within a period of two months. The procedure was suspended for a total of 45 days and extended by one week. Thus, the Opinion must be rendered no later than 9 July 2007.

Ex post prior checking. The processing operations had started before the EDPS was notified. Indeed, the Notification refers to activities which have been already in force in OHIM for several years. Therefore, the prior checking should be considered "ex-post" prior checking.

Since prior checking is designed to address situations that are likely to present risks, the opinion of the EDPS should normally be requested and given prior to the start of the processing operations.

Taking into account that a large number of processing operations were already in place before the EDPS was established and became fully functional in the year 2004, these prior checking

operations, by definition, have to be carried out ex-post. For these reasons, the EDPS does not view the delay with the submission of the Notification as an insurmountable problem in the current case, provided that all recommendations that EDPS makes in this Opinion will be fully taken into account.

2.2.2. Lawfulness and proportionality of the processing

Article 5(a) of the Regulation provides that personal data may be processed if "processing is necessary for the performance of a task carried out in the public interest on the basis of the Treaties ... or other legal instrument adopted on the basis thereof".

The first issue under Article 5(a) is to determine whether the processing is instituted to serve a specific public interest task provided for in a Treaty provision or another legal instrument adopted on the basis of the Treaties. The second issue is to determine whether the processing operation is indeed necessary for the performance of such a task.

To address the first issue in the present case, Recital 27 of the Regulation needs to be taken into account, which specifies that "processing of personal data for performance of tasks carried out in the public interest includes the processing necessary for the management and functioning of those institutions and bodies". Taken together, thus, the issue in the present case is whether the processing is necessary for the management and functioning of OHIM.

OHIM is a Community body, and the granting of social financial aid forms part of the management of its own internal activities. Processing data in order to provide social financial aid to staff members is an activity that is included within the broad term of "processing necessary for the management and functioning of" OHIM. Indeed, granting this type of aid is specifically authorized in Article 76 of the Staff Regulations. In case of the disability aid, the processing is further regulated in the OHIM Decision described in Section 2.1.3 above.

Based on the foregoing, the EDPS does not question the lawfulness, proportionality, and legal basis of the notified processing operation.

2.2.3. Processing of special categories of data. Processing of personal data concerning health is prohibited unless grounds can be found in Article 10(2) or 10(3) of the Regulation. As they constitute exceptions to the general prohibition, these Articles must be interpreted narrowly.

As explained above concerning the legal basis, the justification for processing health data in connection with granting social financial aid can be found in Article 76 of the Staff Regulations. Therefore, the processing falls under Article 10(2)(b) of the Regulation, according to which the prohibition shall not apply where the processing is "necessary for the purposes 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".

Based on these provisions, the EDPS considers that OHIM's data processing operations are permissible, provided that they are limited to the purposes of granting the requested social financial aid.

2.2.4. Data Quality

Adequacy, relevance, and proportionality. According to Article 4(1)(c) of the Regulation personal data must be "adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed." Based on the facts submitted to it, the EDPS does not question the adequacy, relevance and proportionality of the personal data processed. With that said, the EDPS points out to the importance of a case by case proportionality assessment by OHIM's social worker to ensure that no excessive information is collected for purposes of granting either type of financial aid.

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 (see Section 2.2.8 below).

Accuracy. According to Article (4)(1)(d) 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 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." Based on the facts submitted to it, the EDPS has not found any indication that the processing operations would involve structural defaults which would result in collecting or storing inaccurate data.

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

Considering the requirements of the OHIM Financial Regulation, the EDPS finds the proposed 5-year (as a matter-of fact, up to 7-year) timeline acceptable for all documents necessary for the justification of the correctness of the financial authorization.

With that said, the EDPS specifically calls the attention of the OHIM to a recently added last paragraph to Article 49 of the Implementing Rules of the general Financial Regulation[2], which provides the following: "Personal data contained in supporting documents shall be deleted where possible when those data are not necessary for budgetary discharge, control and audit purposes. In any event, as concerns the conservation of traffic data, Article 37(2) of Regulation (EC) No 45/2001 shall apply." This recent amendment was adopted following the recommendations provided in paragraphs 33-47 of the "Opinion of the EDPS of 12 December 2006 on proposals for amending the Financial Regulation applicable to the general budget of the European Communities and its Implementing Rules (COM(2006) 213 final and SEC(2006) 866 final), OJ C 94, 28.04.2007, p. 12".

2.2.6. Transfers of the data. Article 7(1) of the Regulation provides that "personal data shall only be transferred within or to other Community institutions or bodies if the data are necessary for the legitimate performance of tasks covered by the competence of the recipient."

[2] Commission Regulation (EC, Euratom) No 2342/2002 of 23/12/2002 laying down detailed rules for the implementation of Council Regulation (EC, Euratom) No 1605/2002 on the Financial Regulation applicable to the general budget of the European Communities.

The EDPS welcomes that the use of data is strictly limited to the internal use of OHIM and that the documents containing data regarding the personal circumstances of the data subjects are kept under lock and key either by the social worker or the medical officer. The EDPS also welcomes that OHIM makes considerable efforts to limit the amount of personal data transferred to the finance department.

OHIM explained that sharing certain amount of personal data with the finance department appears to be inevitable when authorizing social financial aid. For example, the finance department must have access to certain data, such as the name of the applicant, his bank account number, and the amount requested. Transfer of such data will mean that the finance department (and those processing the payments) will be aware at least of the fact that a certain staff member had to apply for aid, is disabled, or has disabled family members. In case of the disability aid, the finance department must also be aware of what exact measures (e.g. what transport or housing arrangements) they process payments for. These data may indirectly reveal information about the nature of the disability. Insomuch that these disclosures are strictly necessary and unavoidable, the EDPS finds these transfers acceptable.

The EDPS, however, emphasizes that during any data sharing the amount of data shared must be kept to the minimum strictly necessary. Similarly, the range of recipients of any data must also be strictly limited on a need-to-know basis. In addition, it is also essential that those involved in the processing operation in the financial department must be reminded and trained to be fully aware at all times of their confidentiality obligations. Awareness raising activities must also include an explanation of the special sensitivity of health-related data.

This is crucial for non-medical staff given that, as opposed to trained medical practitioners, they are not bound by the medical secrecy rules on the basis of their professional titles. This means that they are not subject to an external self-regulatory authority in matters of professional ethics, such as a national medical chamber. Neither are they subject to an elaborate set of rules on medical secrecy similar to what is available with respect to medical professionals on the national level. Perhaps even more importantly, medical practitioners received comprehensive training on matters related to medical ethics, including medical secrecy. Indeed, as a result of these factors the knowledge and commitment to medical secrecy of accounting and administrative staff who never received formal training on medical secrecy issues and are subject only to general requirements of confidentiality by virtue of Article 17 of the Staff Regulations[3] that they may only perused in a cursory manner are simply not comparable with the knowledge and commitment of a medical professional who took the Hippocratic Oath.

For these reasons, the EDPS recommends that all non-medical staff with access to medical data (this includes staff in the financial department, the authorizing officer, and the social worker) should receive appropriate and comprehensive training on issues of medical secrecy. They should also be required to acknowledge in writing that they received such training and that they undertake to abide by their confidentiality obligations.

2.2.7. Right of access and rectification. According to Article 13(c) of the Regulation, the data subjects have the right to obtain from the controller, without constraint, 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 a right to rectify inaccurate or incomplete data.

[3] "1. An official shall refrain from any unauthorised disclosure of information received in the line of duty, unless that information has already been made public or is accessible to the public. 2. An official shall continue to be bound by this obligation after leaving the service."

The Notification confirms that OHIM provides access to the files to staff members who should contact the social worker with any access requests, but does not establish any specific arrangements in this respect.

The EDPS welcomes that OHIM allows access to the files without setting any specific restrictions. However, the EDPS recommends that OHIM sets safeguards to ensure that any access requests will be dealt with in a timely fashion and without constraints. This may include, for example, setting a reasonable timeline for the social worker in which to schedule an access visit, or provide copies of documents, and an obligation on the social worker to consult the OHIM DPO should she wish to limit access to any data requested pursuant to Article 20 of the Regulation. When establishing these safeguards, it must also be ensured that access must be allowed for any or no reason at all. Data subjects also cannot be required to specify the purpose of the request.

Finally, the EDPS considers it appropriate that data subjects may exercise their rights of access relating to the application procedure by contacting the social worker. However, arrangements must be made that data available to the finance department and the medical officer also be provided, if requested by the data subjects. To ensure confidentiality of data, access to medical documents must be provided, in any event, through the medical officer, or in a sealed envelope, marked "confidential, to be opened by the addressee only" or similar.

With respect to access to health-related data, the EDPS also calls OHIM's attention to "Conclusion 221/04" of 19 February 2004 of the Collège des Chefs d'administration, which aims at harmonizing certain aspects of access provision across the Community institutions. This document emphasises that access must be provided to health-related data to the maximum extent possible. The document provides, among others, that access should also be provided to data of psychological or psychiatric nature, although, in such cases, access may be granted indirectly, through the intermediary of a medical practitioner designated by the data subject. The document also specifies that access should also be given to the personal notes of the medical professional who carries out the medical check-up; provided that such access may be denied after examination of the circumstances of the given case if limitation of the disclosure is necessary to protect the interests of the person concerned or the rights of others.

The EDPS, however, emphasises that these limitations must not be read to allow arbitrary restrictions on access. The rule must be free and unrestricted access and any limitations must be rare, specifically justified by the circumstances of the case, and strictly necessary to protect the data subject or the rights and freedoms of others under Article 20(c). In addition, the same case by case analysis must be required with respect to data of psychological or psychiatric nature as with the personal notes of the medical professional.

2.2.8. Information provided to data subjects. Articles 11 and 12 of the Regulation require that certain information be given to data subjects in order to ensure the transparency of the processing of personal data.

Timing and format of the data protection notice. Article 11 provides that when the data are obtained from the data subject, the information must be given at the time of collection. For the case when the data have not been obtained from the data subject, Article 12 provides that the information must be given when the data are first recorded or disclosed, unless the data subject already has it. Article 11 applies, among others, to data contained in documents

submitted by the applicant. Article 12 may apply, for example, to the opinion of the medical officer or the note to file.

Content of the data protection notice. Articles 11 and 12 of the Regulation provide a detailed list of information that needs to be provided to data subjects. In essence, the controller must inform data subjects about who processes what data and for what purposes. The information must also specify the origins and recipients of data, must specify whether replies are obligatory or voluntary and must alert the data subjects to the existence of the right of access and rectification. Any further information, for example, the legal basis of processing, the time limits for storing the data and the right of recourse to the EDPS must also be provided if necessary to guarantee fair processing. This may depend on the circumstances of the case. Finally, both Articles 11 and 12 allows certain exceptions from the notification requirement.

Considering that (i) none of the Article 11 or 12 exceptions apply to the facts of the case, and that (ii) in the present case all items listed in Articles 11 and 12 (including the legal basis of processing, time-limits for storing the data, and the right of recourse to the EDPS) are necessary to guarantee fair processing, the EDPS is of the opinion that all items listed under Articles 11 and 12 respectively must be provided in the data protection notice.

Layered notice. The EDPS welcomes that the salary advance application provides a well-drafted and reassuring data protection notice. The EDPS also welcomes the proposal of OHIM with respect to providing more comprehensive notice to data subjects in the future. All three suggestions made by OHIM and described in Section 2.1.5 are fully endorsed by the EDPS.

As a matter of fact, this approach can be described as a layered approach to notice provision.

First, as suggested by OHIM, the EDPS recommends that OHIM completes the currently available information on its intranet with further information. This should include all items under Articles 11 and 12 of the Regulation. Information about the possibility to apply for a salary advance in certain exceptional cases should also be pointed out on the intranet site. The OHIM Decision is already available on the site.

Second, the EDPS recommends that the OHIM Decision and the note of the social worker regarding salary payments should be supplemented to include provisions regarding data protection.

Third, the application for a disability aid, just as the application for salary advance, should include a data protection clause. It is sufficient if this clause only provides the main elements of the notice, as in the case of the current notice on the application for salary advance, provided that the text contains a link to the intranet page where full notice is provided.

Fourth and finally, as proposed by OHIM, the EDPS also welcomes the practice whereby emails would contain a link to the privacy notice on the OHIM intranet.

2.2.9. Security. According to Articles 22 and 23 of the Regulation, 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 unauthorized disclosure or access, accidental or unlawful destruction or accidental loss, or alteration, and to prevent all other forms of unlawful processing.

The EDPS considers that the security measures adopted by OHIM are adequate in the light of Article 22 of the Regulation, provided that confidentiality of communications is guaranteed.

Conclusion

There is no reason to believe that there is a breach of the provisions of the Regulation provided that the considerations noted in Sections 2.2.2 through 2.2.9 are fully taken into account. The recommendations of the EDPS include, most importantly, the following:

- **Recipients and data transfers:**
  - The EDPS emphasizes that the amount of data shared must be kept to the minimum strictly necessary. Similarly, the range of recipients of any data must also be strictly limited to a need-to-know basis.
  - In addition, it is also essential that those involved in the processing operation in the financial department must be made aware of their confidentiality obligations. Awareness raising activities must include an explanation of the sensitivity of health-related data and signing of a declaration of confidentiality.

- **Information to data subjects:**
  - Clear and specific information needs to be provided to data subjects regarding all items listed under Articles 11 and 12 of the Regulation. The EDPS recommends a layered approach to notice provision. This includes a comprehensive notice on OHIM's intranet site, data protection provisions in the OHIM Decision and in the note of the social worker regarding the granting of salary advance, as well as a short data protection notice on all application forms. Linking to the on-line data protection notice from emails is also a welcome practice.

- **Access rights:**
  - Arrangements must be made that data available to the finance department and the medical officer also be provided if requested by the data subjects. To ensure confidentiality of data, access to medical documents must be provided through the medical officer, or in a sealed envelope.

Done at Brussels, on 3 July 2007

Joaquín BAYO DELGADO
Assistant Supervisor