



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 Assistance"

Brussels, 23 July 2007 (Case 2007-171)

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 Assistance". 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. On 21 June 2007 the EDPS requested further clarifications. OHIM responded on 29 June. Finally, on 4 July 2007 the EDPS sent his draft Opinion to OHIM's DPO for comments. OHIM commented on 20 July 2007.

2. Facts

2.1. Scope of the notification: the activities of OHIM's social worker. The notified processing operations involve the activities of OHIM's social worker relating to "social assistance". The OHIM social worker is employed by OHIM's Human Resources Department.

According to the Notification, the processing operations consist of providing professional counselling and information upon request. The activities of the social worker in connection with granting financial aid were subject to a separate prior checking procedure¹.

The main aim of the service is to assist in reconciling professional and private life and to secure the most favourable personal conditions for each individual to develop their potential. The consultation and assessment service of the social worker covers both professional (communication, stress, conflicts, burn-out, etc) and personal matters (adaptation, specific problems, etc). The social worker also provides information on the various resources of both the social services of Alicante and the Community institutions. Consultations may be made on matters relating to family, money, psychological issues, administrative issues, adjusting to the environment and cultural issues, health, conflict management, relationships, and miscellaneous matters. The social worker handles about 300 consultation cases a year.

¹ See EDPS Opinion of 3 July 2007 on a notification for prior checking regarding the granting of "social financial aid", case nr. 2007/0172.

The social worker carries out individual and collective activities in prevention, assistance and, where the need arises, social accompaniment (social "follow-up"). The persons entitled to seek out the services of the social worker include any persons working for OHIM (whether statutory or not), as well as the family of statutory staff members.

2.2. Verbal consultations. Most consultations are carried out verbally, either via a phone conversation or via a face-to-face interview.

The social worker does not record any personal data with respect to the verbal consultations (apart from contact information if necessary to provide further information subsequently), and does not keep paper or computer files about the consultations or other services that she provides, which may contain personal data. OHIM specifically confirmed that the social worker does not take personal notes during the consultations, and relies on her memory alone. As she works alone, she also does not need notes to share the information with others. She records certain aggregate information about her activities, to report to her supervisors. However, these records and reports do not contain personal data.

2.3. Email records. With that said, emails are also used. In fact, emails play an important part for purposes of organization and case management, follow-up of cases, and extraction of statistical data.

Emails are most typically used to: (i) request an appointment, (ii) request information concerning the Spanish public administration, (iii) request information concerning statutory rights (sick leave, leave on personal grounds, JSIS, etc), (iv) request information about services available for children, (v) request reference for a specialist such as a lawyer or a doctor, (vi) thank or comment on the services provided, (vii) keep the social worker informed about the evolution of a case, (viii) or communicate with another professional in connection with a case (e.g. contact the staff member's lawyer, on request of the staff member).

OHIM does not actively solicit email consultations, or encourage that emails should contain a detailed description of the staff member's personal or professional problems. In fact, the social worker is located on OHIM's premises, and is also available on the telephone. OHIM is a relatively small Community body where walk-ins are feasible. The receipt of confidential personal data by the social worker via email is practically unavoidable, while at the same time, it is by no means inherent in the operations. Nevertheless, on some rare occasions, email is the freely chosen means of communication to also discuss the substance of the matter, for example, if the data subject is on leave, retired, or otherwise not available at the premises of OHIM (e.g., tele-workers, family members). Emails related to the substance of cases are, however, rare. Actually, the most sensitive/private the consultation issue is, the less email is used as a communication tool.

The email communications are not used by the social worker to create a structured file on data subjects. With that said, as explained by OHIM, the social worker may access emails to "refresh her memory" should the same staff member consult her again with a new matter or should an existing matter need follow-up. The social worker also uses emails to extract aggregate data from them for the purposes of reporting about her work to her supervisors.

The very first contact in a consultation case is often by email, although the first contact can also be made in person (walk-ins) or by telephone. Emails are also often used by the social worker to confirm the information that she provided in a telephone conversation, or provide additional information. Whereas the total number of annual consultation cases is approximately 300, the total number of consultation-related emails is estimated to be a yearly

average of 1 000. The proportion of email exchanges in the social worker's activities is estimated to be around 30%.

As mentioned above, the purpose (and therefore also the content) of email communications are related to the organization of a case (estimated 90%), much more than to the "substance" of the matter (estimated 10%). "Substance" oriented emails annually probably concern no more than about 5 persons.

2.4. Conservation period. OHIM retains all emails in the context of the social assistance activities of the social worker for five years. The five year period is counted from the end of the calendar year in which the email was received, for practical reasons, to ensure that the social worker does not need to keep track of multiple deletion dates for each individual email received. OHIM explains the need to retain the emails for the five year period by two reasons.

First, since the social worker does not hold any "social file", she needs the emails to "refresh her memory" when a case is subsequently followed up. She may need, for example, to remember names, contact information, or the context in which a staff member requested assistance. This is actually the main purpose of keeping emails up to 5 years.

The social worker confirmed that she consults "old" emails for follow-up purposes about once a week. For example, she may reopen emails related to a case closed earlier to see whether it is the same person who submitted a related request. In addition, OHIM explained that certain persons present cyclic demands at a specific moment of the year, and in such cases, consulting prior emails may be useful.

Second, the social worker needs to extract aggregate data from the emails for purposes of reporting about her activities. OHIM explained that although the statistical purpose is a secondary one, it remains important since the social worker is from time to time asked about the occurrences of specific situations (e.g. "How many cases concern children of the staff?", "How many cases refer to harassment?"). The type or category of questions is difficult to predict and they depend on "trends" or special needs of OHIM in the context of the development of its staff policy.

2.5. Data transfers and recipients of the data. The social worker alone has access to personal data. No other OHIM personnel have access to the data. The social worker works alone, without any administrative support. No transfer of personal data is foreseen, except that references may be made to specialists (e.g., doctors, psychologists, lawyers), upon prior approval of both the data subject and the specialist. In exceptional cases, data transfers may be necessary "to protect the vital interests of the data subject" under Article 5(e) of Regulation (EC) 45/2001 ("**Regulation**"). This, however, has not yet happened in OHIM's experience to date.

2.6. Access rights. OHIM explained that considering that the services of the social worker and any data processing activities are mainly carried out orally, there is no specific procedure to grant rights to data subjects. Nevertheless, OHIM confirmed that as far as the emails are concerned, the data subjects are granted access without delay upon simple request from the data subject to the social worker.

2.7. Information provided to data subjects. The OHIM intranet describes the services provided by the social worker, points out to the confidentiality of service provision, and provides her contact information. In addition, when a staff member consults the social worker

orally, he or she is informed orally about the confidentiality of the consultations and about the fact that the social worker follows a code of deontology (www.ifsw.org).

During the prior checking procedure, OHIM proposed that in the future it could include a data protection notice (i) in all email exchanges (ii) and on the intranet.

2.8. Security. Access to the social worker's computer is password-protected. Standard OHIM security measures apply. Hard-copies of documents, if any, are stored in locked cupboards, with keys available to the social worker only. Should there be a need for transfer of documents containing personal data, the social worker would mark all documents "confidential" in their respective headers, on routing sheets, or on envelopes.

3. Legal aspects

3.1. 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 provision of social assistance 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 remaining questions are whether the processing operation is automated, or at least partly automated, and whether the data form part of a filing system.

The majority of personal data are exchanged verbally, with little or no record being made by the social worker. The information, even when recorded, is not organized into files on specific data subjects. Emails, however, are exchanged and retained for a period of five years.

Despite the fact that the content of the email messages is usually limited to the organizational aspects of the case, it must be considered that OHIM keeps any email exchanges for a period of five years and the social worker, whenever necessary to follow-up on a case, consults these email records. She also uses these records to extract statistical information from them for reporting purposes. As a matter of fact, thus, the social worker uses the email records as a structured filing system, which can be browsed, as necessary, for example, by names of the data subjects, or key words. The social worker's query of her email records may be able to identify, for example, all previous emails exchanged with a particular staff member, or all emails received in connection with stress at work, from multiple staff members. Considering the digital nature of these records and the possibilities of electronic queries, the processing of email records may also be considered as "processing by automatic means". For this reason, the activities of the social worker, taken together, constitute "partially automated processing", and therefore, in the aggregate, come within the scope of Article 3(2) of the Regulation. 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, but not limited to, his or her ability, efficiency, or conduct. The notified processing operations, in particular, the oral consultations, but also some email communications, are intended to evaluate personal aspects relating to the data subject, in particular, his or her financial, social, and family circumstances.

In addition, the Article 27(2) list also specifically includes, under paragraph (a), processing of data relating to health. The notified processing operations 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 58 days. Thus, the Opinion must be rendered no later than 23 July 2007 (being 21 and 22 July public holidays).

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 specific 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.

3.2. 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 provision of social assistance forms part of the management of its own internal activities. Processing data in order to provide social assistance 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 social assistance as described in the Notification is specifically authorized in Article 1(e) of the Staff Regulations of Officials of the European Communities ("**Staff Regulations**").

Article 1(e)(1) provides the following: "Officials in active employment shall have access to measures of a social nature adopted by the institutions and to services provided by the social welfare bodies referred to in Article 9. Former officials may have access to limited specific measures of a social nature." Article 1(e)(3), additionally, provides that "measures of a social nature adopted in accordance with this Article shall be implemented by each institution in close co-operation with the Staff Committee, on the basis of multi-annual proposed actions. These proposed actions shall be transmitted each year to the budgetary authority in the framework of the budget procedure."

Additionally, in the current case, Article 5(a) of the Regulation as a legal basis is complemented by Article 5(d) of the Regulation, which allows processing of data in case "the data subject has unambiguously given his or her consent". OHIM emphasised that all consultations are initiated voluntarily by the staff members (or their family members), who are under no obligation to seek out the services of the social worker.

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

3.3. 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 social assistance can be found in Article 1(e) 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".

Additionally, in the current case, the legal basis for processing of health data is complemented by Article 10(2)(a) of the Regulation, which allows processing of data in case "the data subject has given his or her express consent".

Based on these provisions, the EDPS considers that OHIM's data processing operations are permissible, provided that they are limited to the purposes of providing the requested social assistance, and further provided that data subjects give their express consent for any processing of their health data (e.g. express consent is required for the social worker to contact a specialist on behalf of the data subject).

3.4. 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.

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 3.2). The issue of fairness is closely related to what information is provided to data subjects (see Section 3.8 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 flaws which would result in collecting or storing inaccurate data.

3.5. 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).

As explained in Section 2.4 above, the social worker currently keeps all emails for a five-year period counted as of the end of the year in which the email was received.

The EDPS points out that OHIM has not shown that either the follow-up of cases or the preparation of statistical information would require such a long (as a matter of fact, five to six year) conservation period.

Therefore, the EDPS recommends that OHIM reassesses whether a shorter (perhaps one or two year) conservation period would be sufficient to accommodate the need for follow-up and statistics.

In any event, the EDPS recommends that a specific opt-out possibility would be provided to staff members in the emails sent by the social worker, specifically alerting them that they can request the social worker to delete all email and other information related to them at any time at their request, and warning them that otherwise the normal (one or two-year) retention period applies. This could be integrated into the layered notice provision as discussed in Section 3.8.

In addition, considering the risks to the rights of third party data subjects, who may not even be aware of the processing, the EDPS recommends that confidential personal data relating to third parties, in any event, be deleted from the email communications, as soon as a case has been dealt with and retention of such data is no longer necessary. For example, an email complaining about harassment or bullying by work colleagues, which may contain very delicate, and possibly also not entirely accurate, information related to third parties should only be kept as long as this is strictly necessary for the social worker to handle the case. At

the same time, personal data of third parties, which are publicly available (for example, on the internet, or in the local yellow-pages), such as names and contact information of lawyers or other specialists, may be deleted at a late date, along with the rest of the emails.

3.6. Data transfers. 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." Articles 8 and 9 of the Regulation allow transfers to other recipients under certain conditions.

The EDPS welcomes that as a general rule the use of data is strictly limited to the internal use of OHIM and that no person other than the social worker has access to her emails or to any other document that may contain personal data in connection with her activities.

As an exception, OHIM explained that sharing certain amount of personal data under exceptional circumstances may be inevitable to "protect the vital interests of the data subject". Insomuch that (i) these disclosures are strictly necessary, (ii) the data subject's consent cannot be obtained, and (iii) the disclosure is permissible according to the code of deontology followed by the social worker, 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.

3.7. 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.

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 provide copies of documents.

It is also important to ensure that the social worker should consult the OHIM DPO whenever in doubt about access provision; in particular, whether access should be restricted pursuant to Article 20 of the Regulation. Restriction on access may become a particularly delicate issue if third party data subjects wish to exercise their rights of access whose data the consulting staff member disclosed to the social worker. For example, a staff member may complain to the social worker about bullying or harassment at work, and the names and behaviour of specific work colleagues may be given and described in an email. For these and similar cases, a case by case approach is recommended, which takes into account the confidential nature of the work of the social worker, the code of deontology applicable to the social worker, best practices in the field of social work, as well as the various interests at stake considering the facts and circumstances of the case.

3.8. 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 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 emails sent by the staff member which reveal his or her own personal data. Article 12 may apply, for example, to personal data of third persons contained in emails received from the staff member consulting the social worker.

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 allow 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.

With respect to the cases when information is disclosed to the social worker about third persons (e.g. a staff member complains about work colleagues), it must be considered, whether, and to what extent, information rights should be restricted pursuant to Article 20(c) of the Regulation to safeguard "the protection of the rights and freedoms of others", considering the confidential nature of the social worker's consultative activities.

Layered notice. The EDPS welcomes the proposal of OHIM with respect to providing comprehensive notice to data subjects in the future. The suggestions made by OHIM and described in Section 3.7 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. The information posted on the intranet should also include that the social worker follows a code of deontology, and a link should be made to the internet site where the code is available (www.ifsw.org). Finally, the possibility to restrict the rights of data subjects under Article 20(c) of the Regulation must also be referred to.

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

3.9. 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.

4. 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 3.2 through 3.9 are fully taken into account. The recommendations of the EDPS include, most importantly, the following:

- **Vital interests of the data subject:** Any processing or disclosure solely on grounds of "protecting the vital interests of the data subject" (Article 5(e) of the Regulation) must be limited to processing and disclosures that are strictly necessary, where the data subject's consent cannot be obtained, and the disclosure is permissible according to the code of deontology followed by the social worker. The amount of such data sharing must be kept to what is strictly necessary. Similarly, the range of recipients of any data must also be strictly limited on a need-to-know basis.
- **Conservation period:** The EDPS recommends that OHIM reassesses whether a shorter conservation period (perhaps one or two years) is sufficient to allow for eventual follow-up and extraction of statistical data. In any event, OHIM should also provide an opportunity to data subjects to opt out of the conservation and request deletion of data. In addition, it must also ensure that non-public third-party data are deleted as soon as no longer required in the case at hand.
- **Restrictions under Article 20((1)c) of the Regulation:** Any restrictions under Article 20(1)(c), including, in particular, restrictions on rights of access and information rights must be carefully considered on a case by case basis, taking into account the provisions of the Regulation, the code of deontology applicable to the social worker, the obligations of confidentiality, as well as best practices in social work. When in doubt, and unless in emergency, the social worker must consult the DPO to ensure a common approach.
- **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, and linking to the on-line data protection notice from emails.

Done at Brussels, on 23 July 2007

Peter HUSTINX
European Data Protection Supervisor