Opinion on a notification for Prior Checking received from the Data Protection Officer of the Office for Harmonization in the Internal Market on the Call Center Technology

Brussels, 11 January 2008 (case 2007-583)

1. Proceedings

On 24 September 2007, the European Data Protection Supervisor (hereinafter 'EDPS') received from the Data Protection Officer ("DPO") of the Office for Harmonization in the Internal Market ("OHIM") a notification for prior checking regarding the Call Centre Technology ('the Notification').

On 31 October 2007, the EDPS requested complementary information which was provided on 13 November 2007. On 4 December 2007, the EDPS sent the draft Opinion to OHIM's DPO for comments which were received on 9 January 2008.

2. Examination of the matter

The same data processing operations described in the Notification are performed in two different areas of OHIM activities and are therefore managed by two different entities; the General Affairs and External Relations Department (GAERD) and the Information Technology and Facilities Management Department (ITFMD). Taking into account that the processing operations share the same features, OHIM's DPO decided to submit them in a single notification for prior checking.

GAERD provides users of the Community trade mark and design systems[1] with two services, a switchboard and an information centre. ITFMD provides OHIM staff and external users with a help desk. The activities of GAERD's switchboard and ITFMD's help desk are outsourced to service providers with whom service level agreements have been concluded. The activities of GAERD's information centre are performed by EU officials or assimilated, including contractual and temporary agents (hereinafter 'EU officials').

2.1. The Facts

GAERD and ITFMD monitor the incoming calls at the switchboard, information centre and help desk through the use of an off the shelf software program referred to as "Call Centre Technology". The monitoring provides information about the volume of the calls received, duration, number of calls attended and rejected, etc. The content of the calls is not

[1] Council Regulation (EC) No 40/94 of 20 December 1993 on the Community trade mark and Council Regulation (EC) No 6/2002 of 12 December 2001 on Community designs.

monitored.[2] This Notification refers to the data processing that occurs in the context of the monitoring of these calls.

The ***purpose*** of the data processing is to assess and improve the quality of the services offered as well as to facilitate the planning of activities and the coordination of workflow and teams. In addition, the information from the information centre is used in the annual appraisal exercise insofar as the members of the center are EU officials. Also, the information from the switchboard and help desk is used to assess compliance with the Service Level Agreements concluded with the providers, insofar as these services are outsourced.

The ***primary responsibility*** for the data processing lies within the General Affairs and External Relations Department (GAERD) and the Information Technology and Facilities Management Department (ITFMD).

The data processing operations are mostly of electronic nature and can be summarised as follows:

(i) Real time information as concerns the activity of the voice calls, performance and alarms[3] is collected and stored in a built-in database attached to the Call Centre Technology program. This is carried out through the use of Module 1 of the software, referred to as the *Information Manager Module*.

(ii) The information stored in the built-in database can be seen by the respective EU officials acting as group coordinators (either in GAERD or in ITFMD) who are processing the data on behalf of the respective controllers. Group coordinators use the data as a management tool to organise the teams in accordance with the peak of work in specific period of the day. They also use it to check the compliance with respective Service Level Agreements concluded with respective contractors.

(iii) The Module 2 of the software, referred to as the *Report Manager Module*, produces periodical statistics both at individual level and group level.

(iv) The group coordinator transfers the data to the authorising officer, i.e., the individual who signs the contract with the external contractors and is responsible for the proper execution of the contract. Authorising officers authorise payments to the respective service providers, for which they may need access to personal information. In principle, the services are invoiced on the basis of aggregated statistics which do not contain personal data. Nevertheless, it cannot be excluded that the authorizing officer requests access to personal statistics in order to take a decision of payment on a more informed basis.

(v) The group coordinator transfers the data to respective directors of departments, deputy director and/or head of service for appraisal purposes.

The ***types of data subjects*** whose data is collected include the following: *(i)* EU officials who work for the OHIM information centre (GAERD); *(ii)* staff working for the service providers in particular in the help desk (ITFMD) and switchboard services (GAERD).

---

[2] Except in the context of silent monitoring which was prior checked by the EDPS, see EDPS Opinion on silent Monitoring, Case 2007-128, adopted on 18 July 2007.

[3] Alarm refers to a mechanism offered by the Call Centre Technology software which is triggered when there are too few operators logged into the system compared to the queue of incoming and waiting calls. When this alarm is activated by the system, operators are to react, log into the system and attend the incoming calls.

The *categories of data* collected and further processed include the following**:** *(i) Identification data,* including EU officials and staff member's name and work phone number; *(ii)* data related to the staff member/EU official activity regarding their attendance of incoming calls. This includes real time information showing the status of the servicing person (such as logged off, servicing, idle), status time (i.e., how long the line has been in this status) and the service group. (iii) Statistical information generally for a range period (day, week, month) stating the date and time of availability of a staff member/EU official working for the three services at point, the duration of activity per day, the number of calls received, the number of calls attended, the number of calls rejected, the number of calls abandoned and the average duration of servicing.

As far as the ***conservation*** of the data is concerned, according to the Notification, the information stored in the built-in database of the Call Centre Technology software (real time information as concerns the activity of the voice calls, performance and alarms) are kept for one year. Individual statistics related to EU officials are stored for one year and individual statistics related to non statutory staff members are kept for seven years for budgetary purposes (in accordance with Article 38.6 of OHIM's Financial Regulation). The reports containing the statistics are generated in an html or PDF format. They are stored on a network drive, access to which is restricted to authorised users, which includes the group coordinators and the operators (data subjects concerned).

The data controller may ***transfer personal data*** gathered in the context of the Call Centre Technology to the following types of recipients which are community institutions or bodies: authorising officers to authorise payments as concerns outsourced activities and the directors of departments, deputy director and/or head of service to use for appraisal purposes as concerns EU officials. In addition, the data related to outsourced activities may be sent to the respective service providers who manage the switchboard and help desk in order to allow them to check the compliance of their services with the Service Level Agreements. However, so far only aggregated and anonymous data are transferred to the service providers.

As far as the ***right to information*** is concerned, the Notification explains that data subjects are sent a data protection statement by email on a yearly basis. A copy of the privacy statement providing the relevant information was annexed to the Notification. The information notice contains information on the identity of the data controller, the purposes of the processing, categories of data processed, the recipients of the data, the existence of a right of access and the right to rectify. It also contains the time limits for storing the data and the individuals' right to consult the EDPS.

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 sending a written request (email) to the respective coordinator.

Security measures have been adopted.

2.2. Legal Aspects

2.2.1. Prior Checking

This Notification relates to the data processing operations that take place in OHIM, to improve the quality of GAERD switchboard and information centre and ITFMD help desk. The most relevant of processing operations described in the Notification is the monitoring of incoming calls received in these three services.

This Opinion will assess the extent to which the monitoring of the calls and related data processing operations are in line with Regulation (EC) No 45/2001 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data (hereinafter "Regulation (EC) No 45/2001). This Opinion will not address data processing operations that go beyond this scope. For example, this Opinion does not deal with the appraisal procedures of EU officials which may take place using some of the information collected in the context of monitoring incoming calls nor the eventual monitoring of the content of incoming calls.[4]

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 or which fall within the scope of Community law*"[5]. For the reasons described below, all elements that trigger the application of the Regulation are present here:

First, the monitoring of incoming calls entails the collection and further processing of *personal data* as defined under Article 2(a) of Regulation (EC) No 45/2001. As described in the Notification, the monitoring will reveal, among others, the calls received by individuals working at the monitored services, the duration of the calls, the number of calls attended and rejected, etc.

Second, 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. Module 1 and 2 of the Call Centre Technology software are used to produce information regarding the calls. Group coordinators, authorising officers and directors of departments will use the information for different purposes.

Finally, the processing is carried out by a Community institution, 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 subject 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 EDPS notes that in principle, the main purpose of the processing is to assess and improve the qualities of the services. However, inherent to this goal is the assessment of the performance of the operators who work for the services. In other words, the assessment of the service entails an assessment of the individuals who work for such services. For the services switchboard and the help desk the assessment refers to staff working for external providers to whom the services are outsourced. For the information centre, the assessment refers to EU officials or assimilated and the use of the information for their assessment is carried out in the context of the annual appraisal exercise.

[4] Both data processing operations have already been prior checked by the EDPS, in prior check Opinions 2004-293 for appraisal and 2007-0128 for silent monitoring.
[5] See Article 3(2) of Regulation (EC) No 45/2001.

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 24 September 2007. The two month period within which the EDPS must deliver an opinion was suspended for a total of 49 days to request further information from OHIM and allow for comments on the draft EDPS Opinion. The Opinion must therefore be adopted no later than 14 January 2008 (13 January being Sunday).

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 the performance of a task to be carried out in the public interest ("Legal basis"), and second, whether the processing operations carried out by the data controllers are indeed necessary for the performance of that task ("Necessity test").

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 data processing in point, the EDPS takes note of the following legal instruments: *(i)* Article 43 of the Staff Regulations[6]; *(ii)* the two service level agreements concluded with the respective service providers and *(iii)* OHIM's administrative decision AMD 00-37 OF 9 07-2001 on the adoption of A Code of Good Administration Behaviour.

The legal basis for processing personal information of EU officials for appraisal purposes is contained in Article 43 of the Staff Regulations which states: *"The ability, efficiency and conduct in the service of each official shall be the subject of a periodical report made at least once every two years as provided for by each institution in accordance with Article 110".* This article authorises OHIM to collect information from officials who work for the OHIM information centre in order to assess their ability, efficiency and conduct.

The service level agreement between the OHIM and the service provider operating GAERD switchboard enables OHIM to process data for the purposes of evaluating the performance of the employees and overall quality of the service. In particular, clause 4.4 of the Service Level Agreement which determines the quality criteria says: *"The Office will evaluate the performance in terms of the following criteria: Answering calls within 20 seconds; Missed*

[6] Staff Regulations of Officials of the European Communities, 1.05.2005.

calls; Complaints; Compliance with the switchboard guidelines". Concerning the last criteria, it is added: *"Concept: the correct application of the guidelines, and compliance with the general criteria of courtesy, professionalism, professional vocation and dynamism. Value: the OHIM's coordinator or his deputy may conduct a random check at any time in order to evaluate the quality level of services provided by the Contractor. Each month, a minimum of 20 calls will be evaluated at random and marked according to the agreed evaluation sheets"*. The service level agreement between OHIM and the service provider operating help desk also enables the processing of personal data of the providers' employees for the purposes of evaluating their performance and the quality of the service altogether. In particular, clause 5 establishes that the on-site desk team manager of the provider will provide reports on a monthly basis, showing the performance of the service desk in relation to the agreed service levels agreed.

In addition, Decision No. ADM-00-37 of the President of the Office of 9 July 2001 on the adoption of a Code of Good Administration Behaviour provides a legal basis to process information for the reasons of quality control and training. This will legitimise the collection of information from the three services for the purposes of quality control and training. This Code reads as follows: *"Quality service. The Office and its staff have a duty to serve the Community interest and, in so doing, the public interest. The public legitimately expects quality service and an administration that is open, accessible and properly run. Quality service calls for the Office and its staff to be courteous, objective and impartial"*.

In sum, the legal basis found in the Staff Regulations of Officials of the European Communities, OHIM's administrative decision AMD 00-37 of 9-July 2001 and Service Level Agreements support the lawfulness of the processing operation.

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 monitoring the activity of the voice calls is "*necessary"* for the performance of a task, in this case, the assessment of the services and of the individuals working for them.

The collection of the information described in the Notification appears necessary in order to assess the quality of the three services offered, the GAERD's switchboard and an information centre and ITFMD help desk. Indeed, unless OHIM collects and further processes specific information related to the performance of the service, it will not be able to determine the quality of the services; in this case, whether telephone communications are answered or returned as promptly as possible. Furthermore, the processing of personal data of EU staff is necessary for the purposes of evaluating them in the context of the annual appraisal procedure foreseen in Article 43 of the Staff Regulations. In the case in point, EU staff working for the information centre is likely to be evaluated, among others, for their performance in carrying out their task. It is therefore necessary to collect information that reflects how they carry out their task within the information centre.

In sum, the EDPS is satisfied that the processing described is necessary for the evaluation procedure established by the Staff Regulations and for the purposes of assessing the quality of the services.

2.2.3. 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 collected, identification data and information related to the staff member/EU official activity seems adequate for the purposes sought by the processing, i.e., the performance of the processing and evaluation of EU staff working for the information centre. The type and nature of the services concerned require prompt reaction as a prerequisite to be considered as working properly. Indeed, in the three services concerned, the answering of telephone calls and the returning of calls as promptly as possible are key conditions for the quality of the service. Therefore, in order to assess whether the services work properly, it is relevant to collect information regarding the details of the attendance of incoming calls. This includes the information collected by the Call Centre Technology software, in particular, the real time situation showing the status of the servicing person (such as logged off, servicing, idle), status time (i.e., how long the line has been in this status) as well as information stating the number of calls received, the number of calls attended, the number of calls rejected, the number of calls abandoned and the average duration of servicing.

In sum, the EDPS considers that the information collected from EU staff and employees of the service providers 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. This is further addressed in Section 2.2.7.

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 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"*. From the information provided, the software Call Centre Technology provides reliable and accurate information regarding overall attendance of incoming calls. The reliability and accuracy of this information is also ensured by informing individuals of the monitoring process and type of information collected and enabling them to access such information. Therefore the information will be systematically checked and eventually corrected or completed (see point 2.2.6). The EDPS is of the opinion that this ensures that the data are accurate and kept up to date throughout the process.

2.2.4. 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. Article 37 of Regulation (EC) 45/2001 provides for specific measures as concerns the conservation of traffic and billing data and establishes that it must be erased or made anonymous as soon as possible and in any case no longer than six months after collection. .

The EDPS notes that Article 37 of Regulation (EC) 45/2001 does not apply in this case insofar as the information processed in the context of the Call Centre Technology does not involve traffic data *per se*, i.e. information to establish calls and other connections over the telecommunications network. Therefore, the assessment as to whether the conservation period is appropriate must be made in the light of Article 4(1)(e) of Regulation (EC) No 45/2001.

The storage time of one year that applies to the real time information contained in the Call Centre Technology database as well as to the individual's statistics related to EU officials and assimilated seems appropriate. One year seems an appropriate period to enable OHIM to use the information to assess and improve the quality of the services as well as to facilitate the planning of the activities and workflow. Furthermore, taking into account that the information of EU officials will be used for appraisal purposes which take place on an annual basis, it seems necessary for OHIM to keep this type of information at least for one year. The Privacy Statement addressed to individuals refers to the possibility of printing the content of the Call Centre Technology database in paper reports which may be kept for up to five years. No reasons are given regarding the specific use of the data during this deadline. Taking into account the overall purposes of the data processing as described in the Notification, the EDPS fails to see the need to keep the printouts for period of five years. Taking into account that the information will be used for appraisal purposes which happen on an annual basis, it seems as if a period of two years would be a necessary storage period for print outs. Therefore, the EDPS calls upon OHIM to shorten the maximum storage period for printouts of the Call Centre Technology software database.

In addition, the EDPS has not been provided with convincing reasons that justify the need to keep individual statistics related to staff members working for the service providers for seven years. The EDPS understands that pursuant to Article 38.6 of OHIM's Financial Regulation supporting documents must be kept for a maximum period of 7 years. However, the EDPS questions the need to provide as support documentation the names of the staff providing the service. Whereas for invoicing purposes, particularly to set up penalties, OHIM needs to collect information on, among others, missed calls, complaints etc, it appears unnecessary to keep the names of the staff members. Accordingly, the EDPS calls upon OHIM to examine the possibility to set up a system which does not keep the names of individuals in the supporting documents that must be kept for a period of seven years.

2.2.5. Transfers of Data

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 and privacy statement, information about EU officials is transferred to the directors of departments, deputy director and/or head of service within OHIM. Information about staff members working for the service providers may be transferred to authorising officers. These recipients are Community institutions and bodies. Thus, to the extent that these recipients are not part of the data controller itself, Article 7 of the Regulation applies. This Article requires personal data to be transferred "*for the legitimate performance of tasks covered by the competence of the recipient*". In order to comply with this provision, in sending personal data, the data controller must ensure that *(i)* the recipient has the appropriate competences and *(ii)* the transfer is necessary. In this regard, the EDPS considers that the transfers of EU officials related data to deputy director and/or head of service for evaluation purposes seem to meet the above requirements. The same occurs regarding the transfers of data pertaining to staff members working for the service providers to authorising officers.[7]

[7] In some cases directors are also authorizing officers. Therefore, when they act in this role, they may receive information about staff members working for the service providers for budgetary/financial purposes.

According to the Notification, the data controller may transfer personal data to the service providers who manage the Switchboard and Help Desk in order to allow them to check the compliance of their services with the Service Level Agreements and further invoice the services. Accordingly, such transfers must comply with Article 8 of the Regulation (EC) No 45/2001 if the providers are established in the EU or Article 9 if they are not subject to Directive 95/46. However, OHIM informed the EDPS that currently only aggregated and anonymous data are transferred to service providers. The EDPS welcomes the fact that only anonymised data are sent to the service providers.

OHIM has confirmed to the EDPS that it does not exclude in the future the possibility to communicate personal data to its external providers, in particular if/when the terms of the service level agreement are not respected and the provider needs or wants to identify the weaknesses of the service provided. If this data transfer takes place, Article 8 must be complied with. Pursuant to Article 8 (b) personal data can be transferred if the recipient establishes the necessity of the transfer and the data subject's legitimate interest is not prejudiced.

In accordance with the factual information given above, it appears that in this case the information will be transferred at the request of the service provider in the event it wants/needs to identify the weaknesses of the service provided. In other words, when it has failed to fulfil the conditions of the service level agreement and it wishes to analyse the causes. For the following reason, the EDPS considers that the service providers will have a legitimate need to have such information.

Firstly, taking into account that the service provider has an obligation to fulfil the service level agreement, if a failure of such service occurs, he must have the tools to evaluate the reason for such malfunction. Because one of the reasons for such failure may be that staff working for the service provider is not fulfilling their obligations as expected, the provider must be able to obtain identification information about its staff and the data showing the staff's performance so that he can identify where the problem resides. Secondly, even in those cases where the service level agreement has not been breached, the service provider may have a legitimate need to have such information in order to evaluate its staff. For the same reasons that OHIM uses such information to evaluate EU officials, the service provider may also wish to use the same type of data for evaluation purposes.

If the above data transfers take place to service providers not subject to Directive 95/46 and established in countries not providing an adequate level of protection, Article 9 must be complied with. Pursuant to Article 9 of Regulation (EC) No 45/2001 personal data can only be transferred in the hypothesis foreseen under Article 9.6 or if the transferor of the information (OHIM) adduces adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals (Article 9.7 of Regulation (EC) No 45/2001). Such safeguards may be provided through contractual clauses. For example, such safeguards could be adduced using the standard contractual clauses adopted by the Commission, available at http://ec.europa.eu/justice_home/fsj/privacy/modelcontracts/index_en.htm. In the light of the facts, in this case, it seems that OHIM will not be able to rely on the hypothesis of Article 9.6 of Regulation (EC) No 45/2001 and will have to comply with Article 9.7. To this end, OHIM will have to adduce safeguards, for example, entering into an agreement or similar with the service provider with the purpose of ensuring the protection of privacy and fundamental rights and freedom of individuals.

2.2.6. 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, individuals are recognised such rights and they are informed that they can be exercised by contacting the data controller. In providing access, the data controllers should ensure that access is limited to individual statistics as opposed to group level statistics.

2.2.7. 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, information to data subjects is given in an information notice by email on a yearly basis. The EDPS considers that it would be more appropriate if this information was provided to individuals when they are hired and then again every year. If the information is given on a yearly basis, it may occur that individuals hired immediately after the annual distribution of the information will not receive the information notice until almost 11 months after their starting of activities.

The EDPS also reviewed the content of the information provided in the privacy statement to verify whether the content satisfies the requirements of Articles 11 and 12 of Regulation (EC) No 45/2001. The privacy statement contains information on the identity of the data controller, the purposes of the processing and how the data is processed, the conditions for the exercise of the right of access and the legal basis for the processing operations. Therefore, the privacy statement contains the information required under Articles 11 and 12 of the Regulation.

2.2.8. Security measures

After careful analysis of the security measures adopted, the EDPS considers that these measures are adequate in the light of Article 22 of Regulation (EC) 45/2001.

3. Conclusion

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

- Reconsider the storage periods, i.e. (i) evaluate why a shorter maximum period of two years is not sufficient regarding printouts of the software database; (ii) examine the possibility to set up a system which does not keep the names of individuals in the supporting documents subject to a seven years conservation period.

- If information is transferred to service providers established in non-adequate third countries, ensure compliance with Article 9 of Regulation 45/2001 by adducing safeguards, for example through contractual clauses or similar.
- Ensure that access is limited to individual statistics as opposed to group level statistics.
- Extend the information mechanism to data subjects as described in this Opinion.

Done at Brussels, 11 January 2008

Joaquín BAYO DELGADO
Assistant Supervisor