Opinion on a notification for prior checking received from the Data Protection Officer of the Office for Harmonization in the Internal Market (Trade Marks and Designs) on silent monitoring

Brussels, 18 July 2007 (Case 2007-128)

1. Proceedings

1.1. On 1 March 2007, the DPO of the Office for Harmonization in the Internal Market (OHIM) sent the notification of silent monitoring to the EDPS for prior checking.

1.2. On 8 March 2007, 9 March 2007, 19 March 2007, 28 March 2007, 4 May 2007 and 10 May 2007, the EDPS requested further information to the DPO of OHIM. The answers have been provided on 8 March 2007, 9 March 2007, 20 March 2007, 18 April 2007, 8 May 2007 and 11 May 2007. On 25 May 2007 the draft Opinion was sent for comments to the DPO, and the answer was received on 12 July 2007.

2. Examination of the matter

2.1. The facts

Purpose of the processing

The processing operations consist in the selective monitoring of incoming phone calls processed by the Information Centre Sector.

OHIM's Information Centre Sector provides OHIM's customer with a two levels information service:

- A Switchboard
- An Information Centre

Incoming phone calls are firstly caught by the Switchboard of OHIM. This activity has been recently outsourced. Depending on the subject of the call, the Switchboard puts the call through either to a specific person in OHIM or to the Information Centre, which is competent to address general issues or further put the call through to a specific person in OHIM.

During a "Silent Monitoring" exercise, incoming callers are firstly asked for their prior consent to participate in the monitoring exercise. Upon their consent, a third party, namely the responsible person in the Information Centre Sector, is silently listening to the conversation. While a call is monitored, a background signal is continuously emitted so that both the caller

and the Switchboard or Information Centre are aware that the call is monitored by a third person. The call is not further monitored when it is put through to a specific person in OHIM.

Therefore, the purposes of the processing operations referred to in the present notification for prior check, are to assess the quality of the service provided by the Switchboard and by the Information Centre as follows:

- Switchboard: Quality control and improvement of services in compliance with the Service Level Agreement concluded with the external provider (contractor).
- Information Centre: Quality control, improvement of services, staff appraisal.

The ultimate purpose of this monitoring activity is to improve OHIM's customer satisfaction by providing a high quality service at the Information Centre Sector.

Another purpose of the processing activity is training, in order to ensure a good preparation of new staff members. According to specific needs, for harmonization and training purposes, team members may listen into each other's calls (it has to be noted that the turnover in this sector is very low, as clarified by the DPO. At an overestimated maximum, this sector incorporates an average of two new people per year. This means that the "need" basis is quite rare). No written records are kept. Such exercise is not taken into consideration for evaluation purposes.

This monitoring activity is selective. It is carried out several times a year during several consecutive days. As concerns the evaluation purposes, the monitoring activity is conducted 2 – 3 times / year. As concerns the training purposes as described above, this is done on the basis of need.

Categories of data subjects

The data subjects concerned are the staff dedicated to Switchboard (by the contractor), the staff dedicated to Information Centre (by OHIM), and the incoming callers.

Categories of data processed

The data categories processed in the evaluation reports' form include:

- Name of staff monitored
- Date of monitoring
- Language monitored
- Assessment with regard to the substance of the reply provided to callers
- Assessment with regard to the form of the reply provided to callers
- Assessment with regard to the use of language

Information to be given to data subjects

Prior to the launching of a monitoring exercise, data subjects are sent a notice informing them about this launching and a data protection statement is annexed.

Incoming callers are asked to provide oral consent prior to monitoring. At this point they are given a brief explanation of the procedure and the purposes. They are not forced to accept such monitoring. During the silent monitoring exercise, individuals who call are provided with the following message orally: "We are currently monitoring incoming calls for training and quality purposes which means that a colleague is listening to this call. Is that all right with you?". This

message may be given either in English, French, Spanish, Italian or German according to the language of the caller. Switchboard/Information Centre staff has this standard message on paper close to the phone during the silent monitoring exercise.

Procedures to grant rights to data subjects

The procedures to grant rights of data subjects are described in the proposal for data protection statement, which was added to the notification as annex 4.

When asked by the EDPS about the way by which data accuracy is guaranteed, the controller answered: "The monitored calls are not recorded on any support. Moreover, the evaluation does not aim at scoring the staff, but at making a general appreciation of the way calls are handled. All evaluations are followed by an open dialogue between the evaluator and the data subject in a very short delay, namely the very same day or the day after at the latest. Therefore, it is considered that the nature of the evaluation and the very short delay in which this evaluation is jointly examined by the evaluator and the data subject provides sufficient guarantee of its accuracy. So far, it is considered that the weight of the silent monitoring exercise in the annual appraisal is less than 5%."

Type of processing operation

The processing operations of personal data related to the silent monitoring are partly automated.

Recipients or categories of recipients to whom the data might be disclosed

The data processed might be disclosed to the Head of the Information Centre Sector, the Management of the Department (Director and Deputy Director), and the Coordinator of the Contractor with regard to Switchboard evaluations**.**

Time limits

The time limit for blocking is immediate. In what concerns erasure, it can be immediate as far as relevant during the retention period.

The conservation policy can be described as follows:

Data are kept:

- For 5 years (+2)[1] with regard to Switchboard evaluations in accordance with article 38§6 of the Financial Regulation of the Office ("*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*").
- For 1 year with regard to Information Centre staff, corresponding to the appraisal reference period. This period may be extended in case of appeal in accordance with articles 90 and 91 of the Staff Regulations.

[1] Article 94§2 of OHIM's Financial Regulation reads that "The Budget Committee shall, before 30 April of year N+2 give discharge […]". Therefore, depending on the moment of the discharge, OHIM considers that the retention period may last up to five years +2. Article 94 of OHIM's Financial Regulation also foresees that this period may be extended. In that respect, this provision does not mention any limit. Nevertheless, such extension would be a very exceptional situation and should not be taken into consideration when fixing a retention period for a supporting document related to the implementation of the budget.

Confidentiality of communications

Aside from the official phone number where monitored calls are received, each staff member has a personal one. Only incoming calls at this official phone number may be monitored. The personal phone number can be used to make/receive personal/professional calls during the day. Incoming/outgoing calls to/from the personal number are by no means subject to monitoring.

In addition, since clients (incoming callers) are asked whether they agree to the monitoring, it is expected that if a personal phone call would be in between (which in principle does not happen anyway), the person simply could refuse the monitoring exercise. In that respect, it can be confirmed that, according to the experience acquired, 100% of the calls received at the official phone number and subject to this monitoring exercise are of a professional nature.

Security measures

The reports are stored on a network drive accessible only by the Head of the Information Centre Sector. Standards Windows XP security measures apply.

2.2. Legal aspects

2.2.1. Prior checking

Presence of elements that trigger the application of Regulation (EC) N. 45/2001

The prior checking relates to the processing of personal data in the context of silent monitoring conducted by OHIM (Articles 2(a) and (b) of Regulation (EC) N. 45/2001 -hereinafter "the Regulation"-). The processing activity is carried out by a Community body, in the framework of Community law (Article 3.1 of the Regulation). The processing of personal data is done partly by automated means (Article 3.2 of the Regulation).

Personal data is processed in the context of the evaluation reports. Then, even if, for the time being, data of the incoming callers is not processed, they will also be considered in the present Opinion due to the reasons given below (see point 2.2.3 below).

The processing of the data is carried out by a Community body and is carried out in the exercise of activities which fall within the scope of Community law.

The Regulation applies notably to the processing of personal data conducted otherwise than by automatic means which form part of a filing system or are intended to form part of a filing system. In the case at hand, the files are systematically organised by name of the evaluated person.

The Regulation therefore applies.

Assessment of whether the data processing operations fall under Article 27 of the Regulation

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 of the Regulation contains a list of processing operations that are likely to present risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes, including processing operations intended to evaluate personal aspects relating to the data subject, including his/her ability, efficiency and conduct (Article 27.2(b)). The procedure described above is notably used to make that kind of evaluation. The case therefore clearly qualifies for 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 operation has already been established. In any case, this is not a serious problem in that any recommendations made by the EDPS may still be adopted accordingly.

The notification of the DPO was received on 1 March 2007. According to Article 27(4) the present opinion must be delivered within a period of two months. The time limit was suspended for 77 days. The opinion must therefore be delivered by 18 July 2007.

2.2.2. Lawfulness of the processing and legal basis

Article 5(a) of the Regulation stipulates that personal data may be processed only if the *"processing is necessary for the 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"*. Recital (§27) to the Regulation further specifies that *"processing of data for the performance of tasks carried out in the public interest of the Community institutions and bodies includes the processing of personal data necessary for the management and functioning of those institutions and bodies"*.

In order to determine whether the processing operations comply with Article 5(a) of the Regulation three elements must be taken into account: first, whether either the Treaty or other legal instruments foresee the data processing operations carried out by OHIM; second, whether the processing operations are performed in the public interest and; third, whether the processing operations are necessary. Obviously, the three requirements are closely related.

As far as the first element is concerned, the legal basis for the data processing conducted in what concerns the staff appraisal in the context of the Information Centre monitoring is Article 43 of the Staff Regulations (as applicable in accordance with Article 112 of Regulation 40/94[1]), 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. (...)"*.

Furthermore, the legal basis for the data processing conducted for the reasons of quality control and training in the context of the Information Centre monitoring is 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. This Code foresees as follows: *"Quality service. The Office and its staff have a duty*

[1] *"1. The Staff Regulations of officials of the European Communities, (...) shall apply to the staff of the Office, (...)"*.

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"; "Dealing with enquiries. (...) Telephone communication. When answering the telephone, staff shall identify themselves or their department. They shall return telephone calls as promptly as possible. Staff replying to enquiries shall provide information on subjects for which they have direct responsibility and/or should direct the caller to the appropriate source in other cases. If necessary, they should refer callers to their superior or consult him or her before giving the information. (...)"[1]

A relevant instrument for the data processing conducted in the context of the Switchboard monitoring is clause 4.4 of the Service Level Agreement signed between OHIM and the contractor. This clause determines the quality criteria: *"The Office will evaluate the performance in terms of the following criteria: Answering calls within 20 seconds; Missed calls; Complaints; Compliance with the switchboard guidelines"*. In what concerns 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"*.

As far as the second element is concerned, the monitoring of communications for the purpose of quality control, improvement of services, staff appraisal and training can be considered as being activities conducted in the public interest.

As far as the third element is concerned, the necessity of the processing has to be evaluated in the light of the purpose. In the present case, the processing is, in principle, necessary for the purposes described, except for the training purpose, where other means could be used (see below point 2.2.3). However, considering that the need basis is quite rare (as described in point 2.1 above) the use of other means (such as recording and anonymisation) would require a disproportionate effort as concerns the training of so few staff members, and would involve a not less excessive cost (as pointed out by the DPO when asked in this regard). In the light of these very specific circumstances, it can be therefore considered that listening is also acceptable for the training purpose.

However, the EDPS notes that the "necessity" of the data processing has to be analysed *in concreto,* for each particular case when the monitoring form is filled in. From this perspective, it has to be borne in mind that the processing of personal data to be conducted in the context of the silent monitoring has to be proportional to the general purpose of processing. Thus, the proportionality has to be evaluated on a case-by-case basis.

Article 5(d) of the Regulation states that personal data may be processed, inter alia, if *"the data subject has unambiguously given his or her consent"*. Indeed, incoming callers are asked for their consent before the monitoring of the conversation starts.

It has to be noted that "consent" is a basis for lawfulness of limited use for processing activities conducted in the context of an employment relationship. Indeed, *"[t]he Article 29 Working Party takes the view that where consent is required from a worker, and there is a real or*

[1] Opinion 8/2001 on the processing of personal data in the employment context, Adopted on 13 September 2001, WP 48, page 23. The Articles mentioned in the quotation belong to Directive 95/46/EC.

potential relevant prejudice that arises from not consenting, the consent is not valid in terms of satisfying either Article 7 or Article 8 as it is not freely given. If it is not possible for a worker to refuse, it is not consent. Consent must at all times be freely given. Thus a worker must be able to withdraw consent without prejudice". Considering the above mentioned purposes of the processing activity, consent could not be used, under the circumstances of this case, as an appropriate basis for lawfulness, since the employee is not completely free to withdraw it. However, a nuance should be made as to the listening for training purpose, where the consent not only of the incoming caller but also of the recipient (OHIM or contractor employee) has to be asked for. Indeed, in this case no prejudice could arise to the worker from not consenting, since the trainee could listen to another employee (see point 2.2.4).

The notification form states that the basis for lawfulness of the processing regarding the Switchboard is Article 5(c) of the Regulation, which stipulates that personal data may be processed only if *"processing is necessary for the performance of a contract to which the data subject is party"*. However, the data subject, that is the employee of the contractor, is not a party of the contract under which this monitoring activity is being conducted and under which the processing of personal data is being done. Indeed, the purpose of processing is analysing the quality of the service provided in the context of the contract between the contractor and OHIM. Therefore, Article 5(c) of the Regulation is not relevant in this context. As expressed before, Article 5(a) of the Regulation has to be considered also as the legal basis for the Switchboard, taking in to account the specifications in the Service Level Agreement.

2.2.3. Data Quality

Article 4§1 c) provides that *"data must be adequate, relevant and non excessive in relation to the purposes for which collected and/or further processed"*.

From the six data categories used, three are open fields that may be variable according to the case and may involve subjective comments. Guarantees must be established in order to ensure the respect for the principle of data quality, and limit the comments to those which are adequate, relevant and non excessive for the purposes mentioned in point 2.1. This could take the form of a general recommendation to the staff members of OHIM conducting the monitoring activity reminding them of the rule and recommending them to ensure the respect of the rule.

Regarding the non-excessiveness (which has to be evaluated in the light of the "necessity" *vis-à-vis* the purpose of the processing), the frequency of the monitoring activity has to be considered. It has been explained that "[i]t is carried out several times a year during 5 consecutive days. As concerns the evaluation purposes, the monitoring activity is conducted 2 – 3 times / year. As concerns the training purposes as described above, this is done on a need basis, and would not exceed half a day per person to be trained. The EDPS is of the view that these frequencies are proportionate and respect the data quality principle.

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."*

This principle is very much connected to the exercise of the right of access, rectification, blocking and erasure (see point 2.2.7 below). It has to be noted that it is difficult to guarantee the accuracy of the data processed in the context of the monitoring (the notes taken and the

comments made in the open fields) if no recording is made of the phone call monitored. If the person monitored does not agree with the comments made, there is no evidence for either part (the person monitored and the person conducting the monitoring) to defend their position and sustain the accuracy of the data (e.g. the appropriateness of the appreciation made on the basis of the listened call). Even if the monitoring does not aim to score the staff, it is part of an evaluation procedure, and as such, it should give enough guarantees to ensure the fairness of such exercise. In the case of the Switchboard, the purpose of the monitoring is not evaluation of the staff but quality control. Then, what is being evaluated by the monitoring activity is the quality of the service offered by the contractor, who is a legal person. However, since the service is offered through the monitored persons working for the contractor, and given the fact that the contractor will have access to the results of the monitoring, this activity could have an impact in the employment relationship between the contractor and the person working at the Switchboard. Therefore, the EDPS suggests that OHIM should find a method to guarantee the accuracy of the data. This could be done either by recording the monitored calls or sharing with the data subject the results of the monitoring in an immediate manner (e.g. after each day of the monitoring exercise), in such a way that the results are documented and discussed as soon as possible after the listening.

Data must also be *"processed fairly and lawfully"* (Article 4.1(a) of the Regulation). The question of lawfulness has already been considered. As for fairness, it is related to the information given to the data subjects (see point 2.2.8 below).

2.2.4. Confidentiality of communications

According to Article 36 of the Regulation, *"Community institutions and bodies shall ensure the confidentiality of communications by means of telecommunications networks and terminal equipment, in accordance with the general principles of Community law"*.

The principle of confidentiality of communications can be read in two ways: the Community institutions must ensure the confidentiality of communications from any interference coming from the outside, but also respect the confidentiality of communications themselves. The first is linked to the security of the network (see 2.2.9 below).

Article 36 of the Regulation was inspired by Article 5 of Directive 97/66[1] which notably provides that Member states must prohibit listening, tapping, storage or other kinds of interception or surveillance of communications, by others than users, without the consent of the users concerned, except when legally authorised in accordance with the general principles of Community law. Directive 97/66 has since been replaced by Directive (EC) 2002/58[2], but the principle remains the same: providing the parties to the communication have given their consent, there is no breach of the principle of confidentiality of communications (Article 5 of Directive (EC) 2002/58). The EDPS believes that Article 36 of Regulation 45/2001 must be interpreted along those same lines.

Following the "general principles of Community law" in the present case, it is necessary to analyse whether there is a breach to the confidentiality of communications in order to proceed

[1] Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector.

[2] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and telecommunications).

with the application of the legal rules above mentioned. The practice of silent monitoring is conducted in the following way: the employees receive an in-advance notice informing them when the monitoring will be conducted. The incoming callers are also informed before each exercise. The monitoring is conducted 2 or 3 times a year. Apart from that, only professional calls are received in the monitored telephones, the employees having another phone available in case a personal call has to be done or received. Therefore, it is observed that sufficient guarantees have been developed in the context of the silent monitoring. This allows reaching the conclusion that there is no breach of confidentiality regarding the monitored communications. In what concerns the listening conducted for the training purpose, the consent of both parties of the communication has to be requested (as recommended in point 2.2.2 of the present Opinion)

2.2.5. Conservation of data

According to Article 4.1(e) of the Regulation, 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 are collected and/or further processed.

The conservation periods described in point 2.1 of the present Opinion respect the Regulation. However, in the case of the Switchboard, only data that are necessary for budgetary purposes can be kept for 5 more years after discharge. Otherwise, the retention for 1 year will have to be implemented.

2.2.6. Transfer of data

Transfer of personal data within or between Community institutions or bodies

According to Article 7§1 of Regulation 45/2001, personal data may only be transferred within or between Community institutions or bodies notably *"if the data are necessary for the legitimate performance of tasks covered by the competence of the recipient"*. In the present case, the data is only disclosed within OHIM and to the departments with responsibility over the purposes for which the monitoring activity is conducted. Therefore, Article 7 is respected.

Transfer of personal data to recipients, other than Community institutions or bodies, subject to Directive 95/46/EC

Article 8 of the Regulation stipulates as follows: *"[w]ithout prejudice to Article 4, 5, 6 and 10, personal data shall only be transferred to recipients subject to the national law adopted for the implementation of Directive 95/46/EC, (a) if the recipient establishes that the data are necessary for the performance of a task carried out in the public interest or subject to the exercise of public authority, (...)"*.

The contractor is a private body established in Spain, therefore, due to the application of Article 4.1(a) of Directive 95/46/EC, Spanish data protection law is applicable (national law adopted for the implementation of Directive 95/46/EC). Whereas under Article 8(a) of the Regulation it is up to the recipient to establish the interest, the EDPS understands this provision to mean that if the sending of the information is not carried out at the request of the recipient, is up to the sender to accredit such a need. In the case at hand, the contractor needs to be informed about the results of the monitoring since this company must guarantee the quality of the service provided. This need can be accredited by OHIM. As a consequence, Article 8 is respected.

2.2.7. Right of access and rectification

According to Article 13 of Regulation (EC) 45/2001, *"the data subject shall have the right to obtain without constraint and at any time within three months from the receipt of the request and free of charge from the controller information at least as to the purposes of the processing operation, the categories of data concerned, the recipients to whom the data are disclosed and communication in an intelligible form of the data undergoing processing and of any available information as to their source"*. Article 14 provides: *"the data subject shall have the right to obtain from the controller the rectification without delay of inaccurate or incomplete personal data"*.

The proposal for a data protection statement annexed to the notification form mentions the procedures to grant these rights to the data subject. This statement still has to be implemented, whereas the processing activity is already in place. Therefore, the EDPS emphasizes that those rights (access and rectification) should be respected as to the processing operations that have already taken place, in the same way as described in the proposal for statement.

2.2.8. Right to object

Article 18 of the Regulation foresees: *"[t]he data subject shall have the right: (a) to object at any time, on compelling legitimate grounds relating to his or her particular situation, to the processing of data relating to him or her, except in the cases covered by Article 5(b), (c) and (d). Where there is a justified objection, the processing in question may no longuer involve those data; (...)"*.

The proposal for a data protection statement annexed to the notification form mentions, in the part dedicated to the Switchboard, that "the data subject may not object to the processing operations, should he/she have eventual compelling legitimate grounds relating to his/her particular situation (...)". However, considering that the basis for lawfulness of this processing operation is Article 5(a) and not 5(c), the right to object has to be respected. The EDPS suggests the deletion of the above mentioned part of the statement. Moreover, the EDPS suggests giving full recognition of this right if appropriate, considering it on a case-by-case basis.

2.2.9. Information to the data subject

Article 11 of the Regulation specifies that the controller must provide information to the data subject except where he or she already has it. This information covers at least the identity of the controller, the purposes of the processing operation for which the data are intended, the recipients or categories of recipients, whether replies to questions are obligatory or not as well as the possible consequence of a failure to reply and the existence of a right of access to, and right to rectify the data concerning him/her. Further information may also have to be provided such as the legal basis of the processing operation, the time-limits for storing the data and the right to have recourse at any time to the EDPS. When personal data is collected directly from the data subject, the information should be provided at the time of collection of this data.

The proposal for a data protection statement annexed to the notification form makes a difference between the information to be given in the context of the Switchboard and in the context of the

Information Centre. However, the EDPS is of the opinion that, since the basis for lawfulness in both cases is the same (Article 5(a) of the Regulation), the information to be given does not have to vary in this regard. On the contrary, as far as the information on the purpose is concerned, a difference has to be established.

In what concerns the information to be given to the incoming caller, the EDPS acknowledges the notice provided. Nevertheless, in case the call is recorded, clarification will have to be given in this regard. Furthermore, the complete information foreseen in Article 11 has to be provided on OHIM's website, specifying the context in which the processing activity will take place.

2.2.10. 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. However, special measures will have to be designed for the secure storage of the recorded calls, in case this method is chosen to guarantee the accuracy of the data.

3. Conclusion

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

- avoid the use of Article 5(c) of the Regulation as the basis for lawfulness regarding the processing operation conducted *vis-à-vis* the Switchboard. On the contrary, Article 5(a) of the Regulation has to be used in this regard;
- elaborate a general recommendation to the staff members of OHIM conducting the monitoring activity, reminding them of the data quality principle and recommending them to ensure that it is respected;
- request the consent of both parties to the communication in the case of listening for training purposes;
- find a method to guarantee the accuracy of the data. This could be done either by recording the monitored calls or by sharing with the data subject the results of the monitoring in an immediate manner (e.g. after each day of the monitoring exercise), in such a way that the results are documented and discussed as soon as possible after the listening.
- in the case of the Switchboard, keep during 5 years only data that are necessary for budgetary reasons, otherwise, a retention period of 1 year has to be implemented;
- respect the rights of access and rectification regarding the data processed in the context of past exercises;
- respect the right to object *vis-à-vis* the employees of the contractor and adapt the information notice in this sense;
- correct the information notice regarding the basis for lawfulness;

- add a full notice to the callers to be posted on OHIM's website,
- implement security measures for the storage of the recorded calls, in case this method is chosen to guarantee the accuracy of the data.

Done at Brussels, 18 July 2007

Peter HUSTINX
European Data Protection Supervisor