Opinion on notification of prior checking received from the Sickness Insurance Management Committee in respect of the "Complaints by members" case.

Brussels, 18 January 2010 (case 2009-0070)

1. Procedure

The Joint Sickness Insurance Scheme (JSIS) operates through a Management Committee (the "Management Committee"), a Central Office, Settlements Offices and a Medical Council. The Management Committee is a joint body where meetings are held of the staff representatives appointed by the Staff Committees of each Institution, together with the representatives of the administrations.

This Management Committee deals with all modifications to the rules by means of proposals or opinions, and complaints made by members, it issues opinions and recommendations, as well as proposals relating to the operation of the joint scheme. In particular, the Committee:

- ensures that the rules are applied uniformly;
- examines the financial situation of the scheme, prepares an annual report, sends the institutions any suggestions or useful recommendations;
- proposes or recommends ways of applying the rules;
- issues opinions in the cases specified, principally on complaints by members and on any matter falling within its area of authority.

On 3 November 2008, the Management Committee asked the assistant European Data Protection Supervisor (EDPS) for a meeting in order to discuss data protection issues in connection with the cases handled by the Management Committee. Following this meeting, it was agreed that the Management Committee would send a notification on the data to the EDPS in respect of members' complaints in view of the sensitive data which might be processed, even though no Data Protection Officer was responsible for sending the said notification, the committee acting at Inter-Institutional level.

On 23 January 2009 a notification for prior checking was sent by the President of the Management Committee to the EDPS, regarding the "complaints by members" case. In an e-mail dated 2 February 2009, questions were put to the President of the Management Committee. Replies were provided on 24 April 2009. At the request of the Management Committee on 4 May 2009 (thus suspending the case) a meeting was arranged for 12 May 2009. Further questions were put on 3 June and replies provided on 12 June. Other questions were put on 15 June and replies provided on 25 September 2009. On 2 October, the EDPS decided to extend the one month deadline because of the complexity of the case, in accordance with Article 27.4 of Regulation (EC) 45/2001 (hereinafter referred to as the Regulation). On 5

October other questions were put and replies provided on 19 October. Additional questions were put on 16 November, replies provided on 27 November. The opinion was sent to the President of the Management Committee for his comments on 3 December 2009. The said comments were received on 15 January 2010.

2. Facts

The Management Committee is called upon to give opinions on complaints by members against decisions relating to the reimbursement of healthcare costs given by the Settlement Offices. The Management Committee adopted the latest version of its rules of procedure on 30 April 2009.

Description of the category or categories of persons affected: this procedure concerns members of the JSIS (permanent officials, temporary staff and contract agents, including retired members) and other beneficiaries of the JSIS (spouses, recognised partners, children and dependents), i.e., potentially, 120,915 persons as at 31.12.2007. In reality, the Management Committee handles between 30 and 40 individual complaints each year.

Description of data or data categories:

- As regards the beneficiaries of the JSIS: surname, forename, address, information required for establishing cover, medical data specific to the particular reimbursement contested: simple indication and/or explanation of the pathology which gave rise to the reimbursement in dispute. There is no access to the medical file. There may possibly be an exchange of letters or e-mails between the member and the Settlement Office. There may possibly be an opinion from the medical officer and/or Medical Council.
- As regards the treating physicians, pharmacists, laboratories, etc.: for example surname, forename, address, speciality.

Information intended for data subjects: data subjects are deemed to know that by submitting a complaint, it will be submitted to the Management Committee for an opinion as this is stipulated in the rules.

Procedures guaranteeing the rights of data subjects: no particular procedure currently exists. However, a specific request not to submit certain information or documents would be taken into account, but it never happens. The opinions issued are anonymised, as are the meeting reports.

Automated/manual processing procedures: the procedure is manual, files are prepared by the Settlement Offices and the administration to which the complaint is submitted. They are distributed to the members by the secretariat and then destroyed by each one individually. The data is stored in paper and electronic form (CIRCA, accessed via an individual password: when a member leaves the Committee, his access is withdrawn).

Processing mainly consists of discussing the case and agreeing on an opinion. According to the Management Committee, the opinion given is anonymised, as is the report of the meeting.

The following information is accessible on CIRCA[1] to the members of the "Management Committee" group:

- opinions given by the Committee (on complaints from members or general questions);

[1] CIRCA is an Internet-based application used by the European Commission and other institutions as a collaboration tool for the exchange of documentation and to create and manage working parties.

- reports of meetings of the Committee;
- reports of meetings of the Medical Council. The Management Committee may put questions to the Medical Council and replies are presented in a general manner. These questions may be either of general interest, for example recognising the operational nature of a new treatment and potentially, therefore, its right to be reimbursed, or of particular interest in the event of a complaint submitted to the Management Committee: request by the latter for clarification in understanding the claimant's medical situation, the medical relevance in his case of the treatment which he is claiming. Extracts from reports of Medical Council meetings which are forwarded to the Management Committee and put on CIRCA only contain the general part without the people being identified, and not the restricted part.
- wordings of agreements entered into with doctors' associations, hospitals, …;
- GIP: various versions having led to the final adoption of the GIP;
- management of the reserve: monthly and annual reports from DG ECFIN;
- annual reports from the Management Committee;
- Management Committee rules of procedure;
- joint regulations;
- opinion to the Medical Council and report (limited) of its meetings;
- meetings: meeting files;
- information provided regularly by the DG BUDG regarding the Scheme's financial situation.

CIRCA/the Management Committee is a private group[2] which has been in existence since 2005. Authorisation is ensured by means of a username and password which are requested by the system when someone logs on to the IG. Access is granted by the Management Committee Secretariat solely to members of the Committee and accredited observers (the Head of the Central Offices, the Settlement Offices and the representatives of retired staff).

The content of the meeting file on CIRCA is the same as the paper file, with the exception of certain documents obtained at the last minute which it has not been possible to insert into the paper file and which are placed on CIRCA, or documents distributed as a paper version at meetings. CIRCA must contain a proper copy of the file which the members had available to them at the time of the Committee meeting. The Management Committee believes that it would be inefficient in terms of time and organisation for each person to have to print the whole of the file (several hundred pages) from CIRCA, but CIRCA is necessary in order to be able to consult the documents prior to receiving the paper file, in order to complete it or access other information. CIRCA permits the electronic storage of any document or information relevant to the work of the Management Committee. Access to documents is secured by means of a login and password. The Management Committee insists in particular on identification data which, it maintains, are essential for issuing its opinion in order, still according to the Committee, to be able to check whether the requirements for reimbursement are met and to give its opinion on this subject. It cites, for example, the case of reimbursements claimed by a member, when in

[2] An interest group (IG) is a working party where the members of the IG and/or the users of CIRCA can collaborate by exchanging documents, organising meetings, exchanging e-mails, messages and discussing.

Various different types of interest groups exist:

1. groups which the user can access with a username, a password and an application for membership (**private groups**). They are, therefore, visible and partially or totally accessible solely to their members. The member is authorised by the leader of the IG.
2. groups which are accessible solely with a username and password (no application for membership required: **registered access IGs**).
3. groups which can be accessed by the public (**public groups**).

fact the prescription was intended for a member of his family not covered under the scheme, the case of a declared doctor but whose training was not recognised as medical, or even the need to check memberships in the case of additional reimbursements.

The Management Committee also stresses that the Settlement Office should complete the file submitted by the member so that it can issue an opinion in full knowledge of the facts and with complete objectivity. In fact, often the member does not attach documents which he knows the administration already has. It can also happen that the member does not attach documents which could be unfavourable for him.

Files remain accessible on CIRCA after the meeting at which they are dealt with, without any time limit. This is particularly useful for understanding certain files and for maintaining coherent "case law" within the Committee. Members of the Committee and observers only have access to CIRCA, and therefore to the data, for the period of their term of office on the Committee.

The Head of the Central Office, the Settlement Offices and the representatives of retired staff are not the recipients of the Committee's opinions, although they are aware of them. They attend meetings but are unable to vote.

The recipients of opinions of a general nature are the institutions and staff committees. The recipients of opinions on claims are the institution which referred the matter to the Management Committee for its opinion and the member in question. The recipients of opinions never have access to either CIRCA or the paper file. They receive the opinions in a memo.

Under the terms of the Joint Regulations, the Central Office provides secretarial services for the Management Committee (Article 39.1.c). Furthermore, it issues, prior to the opinion of the Management Committee, in collaboration with the Settlement Office handling the case, its own opinion on any complaint intended for the AIPN in question, a copy of which is sent to the Committee which considers it in its analysis of the case. In this dual role, therefore, the Head of the Central Office must have access to the meeting file. The Heads of the Settlement Offices deal with applications for reimbursement, prior authorisation, etc. and in this capacity, therefore, are aware of what is going on, and indeed it is they who supply the documents to be included in the files. Normally, therefore, they have access to the files themselves.

Furthermore, the Head of the Central Office and the Heads of the Settlement Offices have access to all the data relating to members in the course of their duties within their departments.

Finally, Article 38.5 of the Joint Regulations states that the Committee shall specify in its rules of procedure *"the persons who may take part in the work of the Committee with the right to vote"*. Article 8.4 of the Committee's rules of procedure state that *"Any association of retired staff of the institutions of the European Union recognised as representative by the European Commission may appoint a representative and a deputy to attend the meetings of the Committee, but without the right to vote. These appointments are valid for a period of two years. These representatives must undertake to respect the confidential nature of the Committee's work"*. In order to *"take part in the work"*, as the Joint Regulations specify, both the representatives of retired staff (one holder of the post and one deputy) also have access to the files.

The opinions issued by the Management Committee are consultative. It is compulsory for them to be requested but they do not have any binding force. It should be noted that they are not

intended for *"the JSIS"* but for the administrations (AIPN) and interested parties. The decision on complaints is not, therefore, taken by an organ of the Joint Scheme, but by the institutions.

Finally, opinions on complaints, whilst referring to a specific complaint number so that the administration knows which file they refer to, are, according to the Management Committee, anonymised.

Recipients to whom the data is likely to be disclosed:

- Members and deputy members of the Management Committee.
- Heads of the Central Office and Settlement Offices. The heads of the Settlement Offices take part in the whole of the meeting of the Management Committee as assistants of the Head of the Central Office. They receive the complete file of the meeting including, therefore, the documents relating to complaints other than those of their own Settlement Office. This practice is considered by the Management Committee to be in the interests of the operation of the Committee, on the one hand because additional clarification can be provided by the person responsible for another Settlement Office, who may, for example have come across a similar case or might propose a solution based on his experience, and on the other in order to ensure equality of treatment by means of the uniform application of Management Committee "case law".
- Representatives of retired staff attend the meeting.

Policy for the conservation of personal data: the Management Committee is a statutory body bound by its own rules as set out by the Joint Regulations and the GIP. Article 11 of its rules of procedure refers to Articles 7.3 and 4.1.e) of Regulation no. 45/2001, and states that data may only be processed for the reasons for which it was disclosed and that it cannot be retained for any longer than is necessary, however it is not stated how long this is. Each person is asked to destroy the complaint files within a reasonable period after the opinion has been given. The data remains on CIRCA for an unlimited period, however access to CIRCA/the Management Committee is limited to the period of office of the members of the Management Committee. Blocking and erasure: Article 11 of the rules of procedure states that each person attending meetings of the Committee shall destroy those parts of the files containing information of a personal nature once the reason for which they were distributed has been finally closed by the Committee. In any event, the secretariat shall retain the file as it was submitted to the Committee, at least until expiry of any possible appeals through the courts. Historical, statistical and scientific purposes: not applicable, since no periods are specified.

Measures taken to ensure security of processing: [...]

3. Legal aspects

3.1. Prior checking

The notification received on 23 January 2009 constitutes processing of personal data ("any information relating to an identified or identifiable person" - Article 2.a of the Regulation). The Management Committee becomes aware of medical information in various ways, notably from information provided by the claimant himself or based on information provided by the Settlement Offices, the person therefore being identified. The data submitted are processed by an inter-institutional community body on behalf of the institutions, set up for carrying out activities which fall within the field of application of community law (Article 3.1). Processing is partially automated and the reimbursement files are stored in paper form for inclusion in a

folder. Article 3.2 is therefore applicable in this case. Therefore, this processing falls within the area of application of the Regulation.

Article 27.1 of the Regulation submits for prior checking by the EDPS any "data processing likely to jeopardise in a specific way the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes". Data processing is also referred to in the provisions of Article 27.2.a: "The following processing operations are likely to present such risks: processing of data relating to health ...", which is the case here as it relates to the collection and processing of medical data by the Management Committee and, as such, is subject to prior checking by the EDPS.

In principle, the checking carried out by the EDPS is prior to the implementation of the processing. Otherwise the checking automatically becomes "ex post". This in no way detracts from the desirability of implementing the recommendations made by the EDPS. Official notification was received on 23 January 2009. The case was suspended for 216 days + the month of August + the one month extension + 43 days for comments. The EDPS will therefore give its opinion by no later than 18 January 2010 (24 March plus 259 days' suspension + two months).

3.2. Lawfulness of processing

Article 5.a of the Regulation states that "*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 or in the legitimate exercise of official authority vested in the Community institution*". Under paragraph 27 of the preamble to the Regulation, processing carried out in the public interest includes the processing of personal data necessary for the management and functioning of those institutions and bodies.

All the personal data contained in the complaints submitted by the data subjects are either provided by such persons, or by the Settlement Offices by way of additional information. This information is processed exclusively within the context of the examination procedure by the Management Committee of complaints made by members in accordance with the purposes and objectives of the procedures. The correct processing of complaints presupposes, therefore, that the Management Committee is able to look at all the information required for this purpose, including on medical matters. This means collecting and processing personal data regarding the members and beneficiaries of the scheme and it is necessary for the legitimate carrying out of the activity of the Management Committee, which is why the processing is lawful.

Under Article 72 of the Staff Regulations, any official, or person treated as such, enjoys an autonomous medical insurance scheme in accordance with regulations adopted pursuant to this provision. Based on Articles 25 and 90, any person may submit an application or complaint to his AIPN in application of the Staff Regulations. Under Article 35.2 of the joint regulation relating to sickness insurance cover for officials of the European Communities (JSIS), before making any decision on a complaint made on the basis of Article 90.2 of the Staff Regulations, the AIPN, or, as appropriate, the administration committee must seek the opinion of the Management Committee. The legal basis relies on the articles above, it complies and it supports the lawfulness of the processing.

Finally, in the context of managing complaints by members, the file of the data subject may reveal data classified in Article 10 of the Regulation as "special categories of data". The file reveals health-related information.

3.3. Processing in respect of special categories of data

Article 10 of the Regulation states that the processing of personal data relating to health is prohibited, unless it is justified for the reasons set out in Articles 10.2 and 10.3 of the Regulation. This case relates very clearly to the processing of personal data relating to health.

Paragraph 3 of this same Article states that the prohibition does not apply "*where processing of the data is required for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, and where those data are processed by a health professional subject to the obligation of professional secrecy or by another person also subject to an equivalent obligation of secrecy.*" The issuing of an opinion on the right to reimbursement claimed by the member involves verifying the conditions set by the Regulation, including, for example, that the name of the beneficiary is the same as the name on the prescription, that the date and place of treatment are the same, the "serious" nature of the illness, the nature of the pathology, the absence of any conflicts of interest, etc. The disclosure of medical data by the Settlement Office to the Management Committee may be considered to be necessary within the context of the management of health-care services and in this respect is, therefore, permitted pursuant to Article 10, paragraph 3.

Furthermore, several provisions impose a duty of confidentiality on officials. Article 17 of the Staff Regulations of officials imposes in fact a general duty of confidentiality with regard to any unauthorised disclosure of information of which they become aware in the course of their duties. Additionally, a particular duty of confidentiality is specified within the JSIS for those involved with the system. Thus Article 37 of the JSIS Regulation states that "*those working in the Settlement Offices and the Central Office, members of the Management Committee and anyone attending meetings of the Management Committee shall be bound by medical confidentiality with regard to the information and/or documents to which they have access in the performance of their duties. They shall continue to be so bound after termination of their employment in those offices of the Management Committee*".

Finally, pursuant to Article 38.7, "*the work of the Management Committee shall be secret*". The secret nature of the work and the fact that every person attending a meeting is subject to such secrecy, is set out again in Article 10 of the Management Committee's rules of procedure adopted on 30 April 2009. Thus the prohibition on processing medical data, as set out in Article 10, does not apply.

3.4. Data quality

The data must be "*adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed*" (Article 4.1.c of the Regulation). In accordance with this principle, only data which is relevant to the complaint may be sent to the Management Committee. In this respect, and given the particularly sensitive nature of the data, the EDPS would like to see the disclosure of any personal data to the Management Committee in the context of a complaint, considered and justified in the light of the principle of the relevance and proportionality of the data. Indeed, it seems to the EDPS that as things stand, the Management Committee's opinion on a complaint relating to the reimbursement of medical expenses does not necessarily and systematically require it to know the identity of the claimant.

In fact, in the context of the opinion relating to "ASSMAL - reimbursement of medical expenses"[3], the EDPS had already carried out this analysis insofar as it related to transfers between PMO and the Management Committee. The EDPS had already highlighted that "*the disclosure of identification data to persons who are not doctors does not appear to be necessary in order to give an opinion on procedural and administrative matters. Furthermore, the disclosure of sensitive information, for example the fact that a member of the staff of the EU is suffering from cancer or a mental illness, could be a deterrent to bringing an appeal in the case of legitimate complaints*", but that he was "*aware of the fact that by not knowing the identity of the patient, in theory, the members of the Management Committee may not encounter potential conflicts of interest (for example, if the question under consideration relates to a member of the family of one of the members of the Management Committee). On the other hand, in such cases, the member of the Management Committee could well identify the patient even without having the identification information*".

Nevertheless, by way of an exception to this principle, the Central Office/Settlement Offices, depending on the nature of the case and its analysis of potential conflicts of interest in particular, could send the Management Committee identification data. The EDPS recommends that the identification data is only forwarded by the Central Office/Settlement Offices if the nature of the case so requires.

Furthermore, the data must be *processed fairly and lawfully* (Article 4.1.a of the Regulation). Lawfulness has already been analysed (see above, point 3.2). Fairness, in the context of such a sensitive subject, requires a great deal of attention. It must be linked to the information which has to be sent to the data subject (see below, point 3.8).

According to Article 4.1.b, personal data must be "*collected for specified, explicit and legitimate purposes and not be further processed in a manner incompatible with these purposes*". It should be remembered, however, that data sent to the Management Committee in the event of a complaint, cannot be used for any other purpose and the EDPS is delighted to see this reference in Article 11 of the new rules of procedure adopted on 30 April 2009.

Finally, data must be "*accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they are collected or for which they are further processed, are erased or rectified*" (Article 4.1.d of the Regulation). The exact nature of the data is based solely on the content of the file sent by the Settlement Offices. The data may be accurate and up to date since the person in question may be called upon to supply the data for processing himself. The question nevertheless arises in the case of a complaint file, when it is posted on CIRCA and the data is updated by the person in question. The EDPS recommends the utmost vigilance in order that files on CIRCA are updated at the same time as the data are also updated.

Furthermore, rights of access and rectification must be available to the data subject, as this helps to ensure that the data is kept up to date and to make the file as complete as possible. These rights constitute the second possibility for ensuring data quality. For these rights of access and rectification, see point 3.7 below.

[3] See opinion 2004-238 of 10 July 2007, on the EDPS website.

3.5. Data retention

Article 4.1.e of the Regulation also sets out the principle that data must 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 ".*

Each of the members is asked to destroy the complaint files within a reasonable period after the opinion has been given. The data remains on CIRCA for an unlimited period, however access to CIRCA/the Management Committee is limited to the period of office of the members of the Management Committee.

Whilst the EDPS is pleased that the paper versions of complaint files are destroyed, the period for which data are kept on CIRCA, on the other hand, poses a problem. It is indeed true that access to CIRCA/the Management Committee is limited to the period in office, but the heads of the Central Office and Settlement Offices have access for the periods in which they occupy the positions, which can be well in excess of two years (period in office of the members of the Management Committee). CIRCA/the Management Committee has been in existence now for 4 years. Whilst this limited access is necessary, the EDPS further recommends that a period be established for which data are retained on CIRCA.

In order to comply with the conditions of Article 4.1.e of the Regulation ("*The Community institution or body shall lay down that personal data which are to be stored for longer periods for historical, statistical or scientific use should be kept either in anonymous form only or, if that is not possible, only with the identity of the data subjects encrypted. In any event, the data shall not be used for any purpose other than for historical, statistical or scientific purposes*"), the EDPS recommends that the complete complaint files from the Management Committee posted on CIRCA can be anonymised (or else that a more restrictive access procedure be defined). For the purposes of maintaining consistency in the opinions given by the Management Committee, consultation could be carried out based on opinions published without identifying the persons in question, which will only be kept on CIRCA. In fact, the opinions are not anonymised insofar as it is always possible to reconstitute the link between the file and the data subject. The documents on the files accompanying the complaints could also remain on CIRCA until the rights of appeal have expired, and then be removed from CIRCA.

3.6. Transfer of data

Data received by the Management Committee from PMO and the member are transferred to the members and deputy members of the Management Committee, the Heads of the Central Office and Settlement Offices and to the representatives of retired staff attending the meeting, by means of the paper file and CIRCA/the Management Committee.

The transmission of medical data and the transfer of personal data between Community institutions and bodies, can only take place if the data are necessary for the legitimate performance of tasks covered by the competence of the recipient (Article 7.1 of the Regulation), which is in effect the case pursuant to Article 35.2 of the Community Regulation on sickness cover for officials of the European Communities (see above, point 3.2).

The transfer of personal data to all the Heads of the Settlement Offices (including where the data do not relate to their own institution) can only take place if this is necessary for the legitimate performance of their task. Only the Head of the Settlement Office of the institution in question is in possession of all the data. This shall be examined on a case-by-case basis. Furthermore, these persons are subject to professional confidentiality (see above, point 3.3).

Furthermore, the recipient shall only process the data for the purposes for which they were disclosed (Article 7.3). This provision is inserted into Article 11 of the new rules of procedure of 30 April 2009.

The provisions of Article 7 of the Regulation are complied with.

3.7. Right of access and rectification

Article 13 of the Regulation sets out the right of access - and the arrangements for such right - at the request of the data subject. Article 14 of the Regulation establishes a right of rectification for the data subject. In the same way as the data subject has a right of access, the said person may also modify the personal data directly or have it modified if necessary. The right of access and rectification is granted in accordance with the Regulation, subject to the possible exceptions set out in Article 20, which allows for the right of access to be limited in order to safeguard interests, especially where such a limitation constitutes a necessary measure in order to safeguard the protection of the data subject or the rights and freedoms of others. However, this limitation must be granted on a case-by-case basis.

It should be remembered that no particular procedure currently exists. The opinions given are published without referring to the data subject and are not anonymised (see 3.5 above**)**, nor are the reports of meetings. The EDPS would point out that anonymisation means making it impossible to recreate a link between a file and a person.

The EDPS recommends introducing rights of access and rectification for the persons in question, subject to the exceptions set out in Article 20, both as regards the paper versions and the versions posted on CIRCA, in order to comply with Articles 13 and 14 of the Regulation.

3.8. Information to the data subjects

In accordance with Articles 11 and 12 of the Regulation, a series of information must be sent to the data subject regarding the processing of personal data. This information will be supplied either at the time of collection where the data are collected from the data subject, or no later than when the first data are disclosed, where the data are not collected directly from the data subject. In the course of processing by the Management Committee, no information relating to the processing of personal data is supplied to the data subjects, whether these are members or doctors.

In order to comply with Articles 11 and 12 of the Regulation, an information memo supplied by the relevant AIPNs under Article 90§2 of the Staff Regulations at the time of bringing the complaint, must be drawn up by the Management Committee in order to inform the persons bringing the complaints relating to sickness insurance, of the provisions of Articles 11 and 12 and in particular the recipients for whom the data are intended and the exercising of rights of access and rectification.

3.9. Security

Article 22 of the Regulation states that the controller shall implement 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. In particular, these security measures must prevent any unauthorised disclosure or access.

The Management Committee does not have any security policy in place, other than the login and individual passwords. The Committee's secretariat only sends the file to those persons listed under the heading of recipients and has a nominative trace of these transmissions. No risk analysis has been carried out as it should have been pursuant to the decision taken in August 2006 by the Commission relating to the security of the information systems used by the services of the Commission, the implementing measures for which were adopted in May 2009.

Given the sensitive nature of the data processed by the Management Committee and the platform used for processing (CIRCA), the EDPS asks the Management Committee to set up an appropriate security policy based on adequate risk analysis, within 6 months of this opinion. Otherwise processing will be deemed to be in breach of Regulation 45/2001.

Conclusion

The proposed processing does not appear to entail any breaches of the provisions of the Regulation, provided that the observations above are taken into account. In particular, this means that the Management Committee:

- examines and justifies the disclosure of any personal data to the Management Committee in the course of a complaint, in the light of the principle of the relevance and proportionality of the data.
- only receives identification data from the Central Office/Settlement Offices if the nature of the file so requires.
- updates the files on CIRCA when the data are also updated.
- sets a limit on the time for which data are kept on CIRCA**.**
- anonymises the complete files from the Management Committee posted on CIRCA (or else establishes a more limited access management procedure). Should this not be possible, then only opinions published without any identification may be kept on CIRCA, with the documents in the files accompanying the complaints remaining on CIRCA until the rights of appeal have expired and then being removed from CIRCA.
- establishes a procedure whereby personal data is only disclosed to all the heads of the Settlement Offices (except in the case of the head of the Settlement Office of the institution in question) if it is necessary for the legitimate performance of their task.
- introduces rights of access and rectification for the data subjects, in respect of both the paper versions and the versions posted on CIRCA, in order to comply with Articles 13 and 14 of the Regulation.
- draws up an information note in order to inform the persons making claims for reimbursement or complaints regarding such claims, of the provisions of Articles 11 and 12 of the Regulation.
- carries out a risk analysis and introduces a security policy within 6 months of this opinion. Otherwise, this persistent failure will be seen as in breach of Regulation 45/2001.

Brussels, 18 January 2010

[Signed]

Giovanni BUTTARELLI
Assistant European Data Protection Supervisor