Opinion on a Notification for Prior Checking Received from the Data Protection Officer of the European Medicines Agency ("EMEA") regarding the EudraVigilance database

Brussels, 7 September 2009 (Case 2008-402)

1. Proceedings

On 25 June 2008, the European Data Protection Supervisor ("EDPS") received from the Data Protection Officer of EMEA a notification for prior checking ("the Notification") regarding the data processing operations carried out in the context of the management of EudraVigilance database ("EudraVigilance"), which is under the direct responsibility of EMEA ("EMEA").

The EDPS requested additional information on 18 September 2008, which was complemented with an additional set of questions sent to EMEA on 10 October 2008.

In the meantime, in parallel with the assessment of EudraVigilance for the purpose of this prior checking Opinion, the EDPS started an assessment of the Commission's proposals to adjust the current legal framework for pharmacovigilance in the European Community, which includes EMEA's role regarding EudraVigilance.

On 23 January 2009, staff members of EMEA and the EDPS met to discuss, among others, how EMEA deals with personal data issues, particularly in the context of the management of EudraVigilance.

On 29 January 2009, EMEA answered partially the first set of questions raised by the EDPS on 18 September 2008. In the light of the complexity of the processing operations, on 30 January 2009, the EDPS extended for two months the period within which he has to issue an opinion. On 12 February 2009, the EDPS made an additional enquiry as a result of the information provided by EMEA in its answer of 29 January 2009 and during the meeting on 23 January 2009.

On 22 April 2009, the EDPS published an opinion on the Commission proposals to adjust the current legal framework on Pharmacovigilance.

On 14 May 2009, EMEA provided the remaining information, including the information requested on 12 February 2009 and the information that was missing from the first information request. On 20 July the EDPS sent the draft Opinion to the EMEA for comments which were received on 4 September 2009.

2. Examination of the matter

2.1. The facts

The overall ***purpose*** *of the data processing* is to enable both National Competent Authorities ("NCAs") and EMEA the reporting and evaluation of suspected adverse reactions to medicinal products for human use (referred to as "Individual Case Safety Reports" or simply "ICSRs") during the development and following the marketing authorisation of medicinal products in the

European Economic Area.

The final aim of the reporting and evaluation includes *(i)* the detection of possible safety signals associated with medicinal products for human use; *(ii)* the ability to make decisions based on broader knowledge of the adverse reaction profile of medicinal products. EudraVigilance therefore contributes to the protection and promotion of public health in the EEA.

The primary ***responsibility for the data processing*** lies within the Post Authorization and Evaluation of Medicines for Human Use Unit of the EMEA.

These ***data processing activities*** can be summarized as follows:

1) Collection and sending of ICSRs to EMEA: NCAs collect ICSRs from health care professionals, marketing authorization holders ("MAHs"), sponsors of clinical trials and others ("sponsors"). NCAs currently send ICSRs to EMEA related to cases (suspected serious adverse reactions) that occurred in their territory. MAHs report suspected (unexpected) serious adverse reactions occurring outside the EEA to EMEA. Sponsors of clinical trials report suspected unexpected serious adverse reactions ("SUSARs") to EudraVigilance in line with the "Detailed guidance on the collection, verification and presentation of adverse reaction reports arising from clinical trials on medicinal products for human use" and national legislation.

Since its foundation in 1995 EMEA only accepted electronically submitted ICSRs for authorized medicinal products according of article 29 f of the Community legislation. Only in exceptional circumstances such as electronic transmission system failure, EMEA accepts transmission of reports via fax, but as soon as the system is working, they are entered in EudraVigilance and the paper copy is destroyed.

2) Reception of ICSRs by EMEA: "ICSRs" are sent electronically in encrypted format to EMEA by means of the EudraVigilance gateway. The report senders are checked for authentication and thereafter the reports are decrypted and transferred to EudraVigilance, where they are validated based on a defined set of business rules.

3) Sharing of Information: The EudraVigilance database is made fully accessible to named users at NCAs, while MAHs only have access to the information which they themselves submitted to EMEA.

On 19 December 2008, EMEA published a draft access policy on its website for public consultation. The document shows how EMEA envisages making available the content of the database also to MAHs and health care professionals.

4) Analysis by EMEA: According to EMEA's mission on the protection of Public health, further to the receipt of the ICSRs, EMEA in consultation with its scientific committees may draw opinions on the measures that should be taken.

Data subjects include the following: *(i)* patients (identified by a generic name or initials) and families of these patients whose data has been included in ICSRs; *(ii)* health care professional and lawyers whose data has been included in ICSRs; *(iii)* individuals related to registered organisations which are part of EudraVigilance User Community. This community includes individuals registered as qualified person for pharmacovigilance or responsible person for EudraVigilance, as assigned/nominated by the MAH or sponsors ("QPPV").

The ***categories of personal data*** collected include the following:

Regarding patients and health care professionals: *(i)* identification data, usually patients are

identified by initials and by a personal identification number (including date of birth); *(ii)* contact details of primary sources of information such as healthcare professionals, in rare instances the patient; *(iii)* physical characteristics of persons; *(iv)* medical history, which may include results of laboratory tests, including in some cases family history; and *(v)* other special categories of data that may be processed, including data concerning sex life (for example if the medical history concerns HIV status). The data stored may date back from 1 January 1995.

Regarding people working for the NCAs or MAHs when they are providing the information to the database and QPPV: identification data, including the full name, address details, contact details, identification document (such as passport or alternative identification document).

Data are ***stored*** on-line in EudraVigilance for an indefinite period to allow a full and complete scientific evaluation of the data.

The data controller ***makes available*** the content of EudraVigilance on-line to the following types of recipients, *(i)* NCAs; *(ii)* MAHs (only the data that they have provided themselves);

Authorities in USA (FDA), Canada (Health Canada) and Japan (Ministry of Health, Labour and Welfare) receive data included in EudraVigilance on ***ad hoc*** basis. Authorities in US, Japan and Canada do not have access to EudraVigilance database itself. If they are given access on an ad hoc basis to content of EudraVigilance, this is done according to the rules contained in the exchanges of letters (also referred to 'arrangements') regarding, among others, how to deal with the information exchanged.

As to the ***right to information to individuals*** whose data is included in EudraVigilance, the Notification states that the information is not collected directly from individuals and hence EMEA does not provide them with information.

The Notification does not refer either to the data subjects' rights of ***access and rectification*** and the procedures to exercise them. According to EMEA, this is because the EMEA does not have direct contact with the data subjects.

As far **as *security measures*** are concerned, the following is relevant: [....]

2.2. Legal aspects

2.2.1. Preliminary aspects

This prior checking Opinion assesses the extent to which EMEA complies with Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 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 ("Regulation (EC) 2001/45") when it processes data in the context of the management of EudraVigilance. The analysis of this matter and the related recommendations has been carried out having the following as a backdrop:

First, EudraVigilance data processing operations are carried out pursuant to existing rules on pharmacovigilance, including those that have been further elaborated in subsequent instruments (e.g., decisions and guidelines) issued by the EMEA or the Commission and the EMEA jointly. Some of these rules are currently in the process of being reviewed by decision makers. The EDPS published an opinion on the Commission proposals to adjust the pharmacovigilance rules, including the monitoring of adverse effects of medicinal products. The comments made in this context were "*lege ferenda*"; yet, they are perfectly applicable to the current data processing related to EudraVigilance. Therefore, this Opinion partially reproduces, in the context of the current

data processing, the same or similar arguments and recommendations as those put forward in the EDPS Opinion of 22 April 2009 on the Commission proposals to adjust the Pharmacovigilance legislation.

Second, as further described below, EudraVigilance is a database managed by EMEA, yet its content originates from National Competent Authorities, Market Authorization Holders and sponsors of clinical trials which forward this information to EMEA. Each of these actors is bound by different data protection legal frameworks. In particular, EMEA must comply with Regulation 45/2001. NCAs, MAHs and sponsors must comply with national law implementing Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data ("Data Protection Directive").

Third, NCAs, MAHs and sponsors are data controller with respect to their own data processing activities as providers of information and users of the system. EMEA has the same role as far as its task of managing EudraVigilance. This is because EMEA, in addition to verifying the information received, is also the operator of the system, and it is responsible, for the technical operation, maintenance, and ensuring the overall security of the system. Accordingly, all the actors share responsibilities with respect to the rights of data subjects, under different legal frameworks and to the extent of their tasks. As a result, all the actors can be deemed "joint controllers" for the part of the data processing for which they are directly competent. As further developed below, as joint-controllers of the system (also referred to as co-controllers"), the different entities have to coordinate their compliance efforts.

This prior checking analyses the extent to which EMEA complies with Regulation 45/2001. It does not assess whether entities at national level comply with their national data protection legislation. However, EMEA's compliance with data protection obligations that arise from Regulation 45/2001 is, to some extent, dependent on NCAs, MAHs and sponsors' compliance when they collect and forward the information**. Therefore, it is of utmost importance for the joint-controllers of the system, to ensure the coordination of their compliance efforts.** In this context, they are responsible for ensuring that such coordination takes place. The individuals' rights to data protection and privacy may be jeopardised unless the different controllers coordinate their efforts to ensure that either at the source of the collection or upon uploading the information in EudraVigilance, individuals have been informed about the processing operations. Accordingly, on a number of occasions, this Opinion calls upon EMEA to coordinate its compliance efforts with those of entities at national.

2.2.2. Prior checking

This prior check Opinion relates to the management by EMEA of EudraVigilance, pursuant to Article 57(1)(d) of Regulation (EC) No 726/2004. As outlined above, EudraVigilance is a centralised data processing network and management system. It serves for the purposes of reporting, evaluating and sharing suspected adverse reactions, during the development and following the marketing authorisation of medicinal products within the EC and EEA.

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*". For the reasons described below, all elements that trigger the application of the Regulation are present:

First, the data contained in EudraVigilance includes personal data as defined under Article 2(a) of

Regulation (EC) No 45/2001. In particular, EudraVigilance contains personal data of patients including sensitive data such as medical histories as well as identification related information from QPPVs. Second, the personal data collected undergo *"automatic processing"* operations, as defined under Article 2(b) of the Regulation (EC) No 45/2001. Indeed, the personal information is uploaded in EudraVigilance and made available on-line to a variety of recipients. Finally, the processing is carried out by an agency, in this case by EMEA, which is part of the European Union, 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 in this processing.

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 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 such risks. This list includes, under paragraph (a), the processing of data relating to health. Most of the data processed in EudraVigilance constitutes health data, including medical histories of patients, reactions to medicines, etc. Therefore the processing operations must 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 will be fully taken into account and the processing operations will be adjusted accordingly.

Notification and due date for the EDPS Opinion. The Notification was received on 25 June 2008. Due to the complexity of the system, the deadline within which the EDPS has to issue an opinion was extended for two months. Pursuant to Article 27(4) of Regulation (EC) No 45/2001, the period within which the EDPS must deliver an opinion was suspended for a total of 223 days to obtain additional information and allow the data controller to review the draft Opinion. The month of August does not count in the calculation of the deadline. The Opinion must therefore be adopted no later than 7 September 2009.

2.2.3. 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. The legal grounds that justify the processing operation may be found in 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 a public interest task, and second, whether the processing operations carried out by EMEA are indeed necessary for the performance of that task.

Legal basis. In ascertaining the legal grounds in the Treaty or in other legal instruments that legitimise the processing operations the EDPS takes note of the following:

1) Article 22 and 57(1)(d) of Regulation (EC) No 726/2004 of the European Parliament and of the Council of 31 March 2004 laying down Community procedures for the authorisation and supervision of medicinal products for human and veterinary use and establishing a European Medicines Agency;

2) Various articles of Directive 2001/83/EC of the European Parliament and of the Council of 6 November 2001 on the Community code relating to medicinal products for human use;

3) Guidelines on Pharmacovigilance for Medicinal Products for Human Use;

4) Directive 2001/20/EC of the European Parliament and of the Council of 4 April 2001 on the approximation of the laws, regulations and administrative provisions of the Member States relating to the implementation of good clinical practice in the conduct of clinical trials on medicinal products for human use.

In addition to establishing EMEA, the above legislation requires the operation of a pharmacovigilance system in which information *"necessary to monitor the safety of medicines and to protect public health"* is collected. Furthermore, the legislation clearly gives EMEA the tasks of ensuring the dissemination of information on adverse reactions to medicinal products authorised in the Community by means of a database. The final goal is for EMEA to take the appropriate measures. EudraVigilance was created to carry out these assignments. In the light of the above, the EDPS has no reason to believe that the above legal framework does not legitimise and give legal basis for the collection of information of adverse effects and their further processing in EudraVigilance.

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. So, the necessity of the data processing is directly linked to the purpose that such processing intends to achieve. In this case, the overall purposes of EudraVigilance is to detect safety signals associated with medicinal products and be able to take the appropriate actions.

The EDPS understands that in order to fulfil the above task it is necessary for EMEA to engage in processing of personal data. In this context, the requirements for compliance with Article 5 a) of Regulation (EC) No 45/2001 are satisfied. This being said, as further explained below under Section 2.2.5 on the "data quality principle", the EDPS is not yet convinced that *all* the personal data and *all* data processing operations carried out in the context of EudraVigilance are indeed necessary for the purpose at stake. Although he fully understands the reasons for the need to collect and further process some personal data, he has concerns as to whether all the venues have been explored, by EMEA together with NCAs and other relevant partners, in order to minimize the processing of personal data to what is really necessary. Furthermore if all the information is indeed necessary, at all the stages, the EDPS is of the view that EMEA should properly explore and report to the EDPS on the possibility to pseudoanonymise the information contained in ICSRs. In this regard, he would like to see EMEA and NCAs to investigate the possibilities for pseudoanonymisation and the application of an harmonized approach to the collection and further processing of personal data.

Taking the above into account, the EDPS is of the view that whereas generally speaking the data processing appears to comply with Article 5(a) of Regulation, this statement must be nuanced in the light of the above comments which are further described under Section 2.2.5.

2.2.4. Processing of special categories of data

Processing of personal data concerning health is prohibited unless grounds can be found in Articles 10(2) and 10(3) of the Regulation. Article 10(2)(a) of the Regulation establishes that the prohibition shall not apply where "*the data subject has given his or her express consent to the processing of those data*". Article 10.3 establishes that the prohibition does not apply if "*the processing is required for the purposes of preventive medicine, medical diagnosis... where those data are processed by a health professional*

subject other obligation of professional secrecy or by another person also subject to an equivalent obligation of secrecy". Similar provisions exist in national laws implementing the Data Protection Directive. In addition, national laws implementing the Data Protection Directive and Article 10.3 of the Regulation foresee that health data may be processed in the context of preventive medicine "*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*".

EudraVigilance contains health related data of patients collected from NCAs and MAHs. EMEA, NCAs and MAHs share responsibility regarding the need to have proper legal grounds for the processing of such data. Pursuant to national laws implementing the Data Protection Directive, the collection and further processing in the context of EudraVigilance of health data at national level may be justified based on the need of this processing in the context of preventive medicine, to avoid the repetition of adverse effects derived from certain medicines on a large scale basis. EMEA's data processing could also be based on the same grounds *ex* Article 10.3 of the Regulation insofar as EMEA's processing fulfils the same role.

The application of Article 10.3 of the Regulation and similar exceptions existing under national law require that all the health related data to be provided is "*required for the purpose of preventive medicine*". This is setting a high standard. If the health information collected from patients is not required but somehow unessential, then the exception would not apply. This means that for this exception to apply it is necessary for all data controllers involved to ensure that the health related data inserted in ICSRs is absolutely necessary. This argument confirms the point that is further developed under Section 2.2.5 on the need to ensure adequacy of the data.

If EMEA and data controllers at national level wish to insert information that is not necessary for the purposes of preventive medicine, on the basis of both Article 10. 2(a) of Regulation (EC) 45/2001 and national laws implementing the Data Protection Directive, additional legal grounds are necessary. Of the remaining legal grounds, consent of individuals appears to be the only available one. Therefore, to collect and or further process information not necessary for preventive medicine, it is necessary to obtain *explicit consent* from the patient. Obviously, it is not necessary for patients to consent twice (for the collection and for the input in EudraVigilance). When NCAs or MAH request consent for the collection of such information, they may request consent *also* for the transfer of such information to EMEA, the input of such information in EudraVigilance and its further dissemination to those who have access to EudraVigilance.

If consent for the initial collection and further processing in the context of EudraVigilance has not been obtained when the data are first collected by NCAs or MAHs, then EMEA will have to obtain such consent, unless EMEA relied on the exception ex Article 10.3 of the Regulation. If so, it will depend, on a case by cases basis, on the information included in the ICSR. The EDPS understands that EMEA has no direct relation with patients and that it would be difficult and sometimes not feasible for EMEA to contact patients in order to obtain their consent. To address this problem, it is crucial for EMEA to cooperate with NCAs and MAHS so as to ensure that NCAS and MAHs only send health data of patients who have previously consented or data that it is necessary for the purposes of preventive medicine and which can therefore be processed without explicit consent.

The above has to be read in conjunction with the comments made in section 2.2.5 regarding the need for pseudoanonymization. The need to obtain patient's consent will be reduced if the information included in ICSRs is pseudoanonymized or anonymized.

2.2.5. 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 they are collected and/or further processed. This is referred to as the data quality principle.

As to the **information contained in EudraVigilance which concerns individuals working for the NCAs or MAHs**, the EDPS does not have any reason to believe that identification related information (name, date of birth, ID/passport), address and phone number are excessive. Taking into account the need to ensure the need for univocal and personalised identification of users, the type of information required seems appropriate. Nevertheless, information such as height, eye colour, pseudonym and children seems to be excessive in reference to the purpose of the processing, i.e., the registration of EudraVigilance users. The EDPS understands that this information is included in some of the national ID cards and that EMEA records them because it is included in such documents. The reason why they keep them, as stated is "*because is the unique identification of the user registered with EV and we need to prevent unauthorised access to EV data in both EVPM and EVCTM. We keep the records as long as the organisation is registered...*" Whereas the EDPS accepts the recording of this information, he considers that as soon as the user registration process is finished, including the identification and checking of the information included in the ID card or passports, EMEA has the option to return, destroy the document or hide the excessive information.

Regarding patient related data, as stated in the Notification, the ICR does not mention patients by name. However, in some instances, a specific patient number is given to each patient, which implies that the system as a whole allows for the traceability of the person involved. Even without the number, in some cases the patient may still be identifiable by combining different pieces of information in the ICSRs.

EMEA has stated, in different occasions, that the collection and further input in EudraVigilance of personal information is necessary for a variety of purposes. This includes the need for traceability (i.e., the verification of the true existence of the patient/reporter), which also includes the need to avoid duplications of ICSRs, the potential need for follow-up and the need for clinical assessment of the reports.

The EDPS fully understands the above reasons which are fully legitimate. However, he is not convinced that appropriate efforts has been made in order to (a) analyze and ensure that only information that is necessary is collected and further processed and, **more particularly to (b) investigate the possibilities for anonymisation or pseudoanonymisatin of ICSRs, notably, in the stage of uploading in EudraVigilance.**

This concern was already raised in the EDPS Opinion of 22 April 2009 on the Commission proposals to adjust the pharmacovigilance framework, where the EDPS wondered whether the processing of health data about identifiable natural persons is actually *necessary* at all stages of the pharmacovigilance system, in particular at the moment when EMEA has to input this information into EudraVigilance.

This concern is corroborated when one reads the following statement included in EudraVigilance Access Policy, which clearly foresees the use of EudraVigilance with anonymised or pseudoanonymised data: "*According to the draft document regarding EudraVigilance Access Policy, the system "should operate on the basis of anonymised reports, in a way that it is not possible to identify the patient' s identity. Appropriate rules regarding the anonymisation of data should be put in place to reach an harmonised approach with all stakeholders [...] This refers in particular to patient information (such as the patient's name, date of birth, cause of death) or other identifying details especially with regard to case summary and additional information provided in adverse reaction reports*". Furthermore, the above is also supported by the

current practice of some NCAs, which on the basis of national laws implementing the Data Protection Directive, do not provide personal identification in the ICSRs. Yet, it is unclear whether this has caused problems for the overall working of the EudraVigilance.

The EDPS accepts that, in particular, in earlier phases of the data processing such as when the data is collected, it may not be possible to exclude the processing of identifiable data. He concedes that in certain, *ad hoc* cases, the need for personal data may exist also in later stages, including when the data is uploaded in EudraVigilance. However, the need for identifiable personal information at later stages, when the data must be recorded in EudraVigilance and particularly when it is shared with other stakeholders, in most cases, is much less clear. In this context, one may wonder whether pseudoanonymised information would not be sufficient.

In order to comply with national data protection legislation and Regulation (EC) No. 45/2001 particularly regarding the data quality principle, EMEA, together with NCAs and other co-controllers ought to examine the above questions with some depth. In particular, the EDPS considers that the extent to which the collection and further processing of personal data in different steps could be limited, should be evaluated. Moreover, EMEA together with NCAs and other co-controllers should carry out the necessary efforts to ascertain whether the use of pseudoanonymised information in ICSRs would be sufficient to fulfil the same purposes. By applying the data quality and minimisation principles in the context of well defined procedures, the EDPS is of the view that in many cases, it might be possible to obtain, if not full anonymity, at least pseudoanonimity. The application of such principles and the setting up of appropriate procedures should not be done by EMEA alone; instead, these efforts should be carried out together with NCAs or MAHs in the context of the initial collection of data. In this context, the EDPS calls upon EMEA, in coordination with NCAs, to consider the following:

First, engage in an investigation of the personal information that is necessary for ICSR forms taking into account the data minimisation/data quality principle. In doing so, one should aim at collecting only the personal data that is necessary. The resulting ICSR form should be accompanied by recommendations as to how it should be completed in order to minimise the use of personal data.

Second, the above should go together with an investigation of the possibilities to anonymise or pseudoanonymise personal information. EMEA together with NCAs or MAHs should endeavor to engage in an evaluation of the extent to which and how the data included in ICSRs could be anonymised or pseudoanonymised. In cases where there is a real need to process identifiable data or when the data cannot be rendered anonymous, EMEA should do its utmost to implement technical possibilities for indirect identification of data subjects, e.g. by making use of pseudonymisation mechanisms.

Third, ensure that, at the different levels, data controllers engage in a 'quality check' of the data. In the same way as the different controllers verify the accuracy of the information (see below sub-section "Accuracy"), they should also 'build in' the procedure the need to carry out a quality of data assessment in order to be able to input ICSRs in EudraVigilance.

It should be recalled that the processing of health related data is subject to a high standard as far as the principle of adequacy is concerned, meaning that only data that is really necessary to fulfil the intended purposes must be collected. This is even more obvious in the case when, as pointed out above, the processing of health related data is not based on consent but on the exception of Article 10.3, which explicitly requires the data to be processed when that is "necessary". In sum, the use of identifiable data should therefore be reduced as far as possible and prevented or stopped at the earliest stage possible in cases where this is not deemed necessary. At this stage, the conclusion can only be that compliance with the requirements of necessity and

proportionality in Articles 4(1)(c) and 10.3 of Regulation (EC) No. 45/2001 is dependent on the outcome of the above actions towards ascertaining the possibilities for anonymisation, pseudoanonymisation and limitation of the data processed.

Fairness and lawfulness. Article 4(1)(a) of the Regulation requires that data 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, which is further addressed in Section 2.2.8.

Accuracy. According to Article 4(1)(d) of the Regulation, personal data must be *"accurate and, where necessary, kept up to date",* and *"every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed , are erased or rectified"*. EMEA and all the actors involved in EudraVigilance have a great interest in the accuracy of the information provided in ICSRs. Towards this end, pursuant to the Guidelines on Pharmacovigilance for Medicinal Products for Human Use, it appears that different rules and provisions that apply to the different stages of the data processing aim at ensuring the accuracy of the information to be reported. In the light of the existence of these procedures aiming at obtaining the most reliable information, the EDPS has no reason to consider that the accuracy principle is not respected.

2.2.6. 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.

Pursuant to the Notification, data are kept for a non-defined period of time to allow a full and complete scientific evaluation of the information.

The EDPS understands the above policy as apparently intended to maximise EMEA's tasks towards protecting safe and effective medicines and the overall role to promote health and wellbeing. On the other hand, the EDPS wonders whether the reasons for keeping personal identifiable information remain for an unlimited period of time in all cases, and even after the decease of the patient. In this context, the EDPS invites EMEA to consider the appropriate length of time during which the information will remain useful for the purposes sought by the data processing. In doing so, EMEA should focus on the real purposes of keeping the data and should take into account the sensitive nature of the information. In this context, the use of pseudoanonymisation or anonymisation tools would be particularly welcome because it would render unnecessary the need to delete the data after a certain time.

2.2.7. 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)* recipients subject to Directive 95/46 (based on Article 8), and *(iii)* or other types of recipients (based on Article 9).

According to the Notification the information is shared with recipients that fall into the categories (ii) and (iii) above.

Before engaging in an assessment of the legal grounds for the transfer of personal information, the EDPS wants to recall what has been said in Section 2.2.5, because it has a direct impact on

the issue of data transfers.

As pointed out above, the EDPS takes the view that the need at general level to include personal data as such into EudraVigilance has not been established. While in some specific cases, it might be necessary and unavoidable, the need of a broader use of personal data appears unproved. If EMEA implements a policy whereby the use of personal data uploaded in EudraVigilance is seriously limited, then, the application of the obligations described below should also be nuanced accordingly.

Transfers to competent Member State authorities (NCAs) subject to Directive 95/46/EC *ex* Article 8 of Regulation (EC) No 45/2001

Regarding transfers to category (ii), the EDPS notes that information is shared with NCAs. As further explained below, this sharing of information with NCAs must comply with Article 8 of Regulation (EC) No 45/2001. In addition, MAHs are given access but only to the information which they themselves submitted to the EMEA; therefore, currently there is no proper sharing of information with MAHs. However, EMEA is considering giving access to MAHs to the rest of information contained in EudraVigilance. If this were to happen, EMEA will have to comply with Article 8 of the Regulation (EC) No 45/2001, which governs the transfers of data to recipients subject to Directive 95/46.

Article 8 of Regulation (EC) No 45/2001 offers several legal grounds authorising the transfer of personal information. Given the circumstances of EMEA's data processing, EMEA may avail itself of Article 8 (a) according to which personal data can be transferred if the data will be used to perform a task subject to public authority or if the data transfer is made in the data subject's legitimate interest. Whereas under Article 8 (a) of Regulation (EC) No 45/2001 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, it is up to the sender to accredit such a need. If this occurs, EMEA may have to re-submit the data processing operations for review.

In accordance with the above, when the information is not sent at the request of the recipient, EMEA must accredit the necessity of the data transfer. The EDPS understands that there is a permanent need for the recipient to be provided with this information as it becomes available. This need has been reflected in the regulatory framework mentioned under Section 2.2.2. In particular, Article 57(1)(d) of Regulation (EC) No 726/2004 which states that EudraVigilance should be permanently accessible to all NCAs. In the EDPS' view, this is sufficient to establish the existence of an interest in having this information.

Of course, the above applies with the remarks made above in Sections 2.2.4 and 2.2.5., stating the need to process sensitive data only when absolutely necessary. Hence, reliance on Article 8 (a) is legitimate to the extent that the amount of health related data transferred is limited to what is absolutely necessary.

Transfers of personal data to recipients other than Community institutions and bodies, which are not subject to Directive 95/46/EC ex Article 9

Regarding the sharing of information with category *(iii)* recipients, EMEA shares information with relevant health authorities as follows: Canada (Ministry of Health), Japan (Ministry of Health, Labour and Welfare) and USA (Federal Drugs Administration). Data shared includes data on adverse reactions which may include personal data. EMEA has exchanged letters with representatives of the Ministries of the three countries.

Prohibition of data transfers and Commission's adequacy: Article 9.1 of the Regulation stipulates that

"[p]ersonal data shall only be transferred to recipients, other than Community institutions and bodies, which are not subject to national law adopted pursuant to Directive 95/46/EC, if an adequate level of protection is ensured in the country of the recipient or within the recipient international organisation and the data are transferred solely to allow tasks covered by the competence of the controller to be carried out".

The European Commission is competent to determine, on the basis of Article 25(6) of the Data Protection Directive whether a third country ensures an adequate level of protection by reason of its domestic law or of the international commitments it has entered into.

The legislation or international commitments that apply to the recipients of the data sent by EMEA - i.e. cases of Canada, Japan and the United States - has not yet been deemed to ensure an adequate level of protection by the European Commission.

Determination by the data controller of the level of protection of the particular transfer to each of the three Ministries: Pursuant to Article 9.2 of the Regulation (EC) 45/2001, EMEA, as data controller, is in a position to carry out an assessment of whether, for the specific transfer of data to the Ministries of Health of the three countries, the transfer provides an adequate level of protection. In doing so, EMEA must assess all the circumstances surrounding the transfer: the nature of the data, the purpose and duration of the processing, the type of recipient, the rules of law, both general and sectoral, and the professional and security measure which are complied in that country. It is suggested to maintain a written record describing the assessment and its outcome.

EMEA has not informed the EDPS of whether it has carried out such assessment and the conclusions it has reached. If EMEA carries out such assessment, it may want to take into account the following:

First, whereas legislation or international commitments of these countries have not been considered adequate by the Commission, it may be useful to take into account that such legislation exists and would apply to the data transferred to these countries as follows:

Japan.- Since 2005, Japan has data protection legislation (The Personal Information Protection Law). However, it does not apply to state institutions, local public bodies, and independent administrative agencies. Such public entities are instead subject to the Act on the Protection of Personal Information Held by Administrative Organs (Act No. 58 of 2003, as amended). For example, Act No 58 of 2003 recognises the right of access but it does not include other EU safeguards.

Canada. - The Canadian Personal Information Protection and Electronic Documents Act, PIPEDA Act, has been deemed as adequate but it only applies to the private sector. It does not apply to the public sector. At the federal level, the Privacy Act regulates collection, use and disclosure of personal information by federal government institutions. These laws provide individuals with a right of access to personal information held by those agencies, but it does not include other EU safeguards. The Act also sets out the mandate and duties of the federal Privacy Commissioner, who is responsible, among others, for enforcing the Act. The Commissioner has suggested reforming the Privacy Act.

United States. - The so-called Safe Harbour principles have also been deemed to provide an adequate level of protection. However, the USA FDA of the US Department of Health and Human Services is not covered by the Safe Harbour principles, (i.e. it is not eligible). The protection of personal information by the federal government is regulated mostly by the Privacy Act of 1974 and the Computer Matching and Privacy Act. The Privacy Act was adopted both to protect personal information in federal databases and to provide individuals with certain rights

over information contained in those databases (right of access). Central oversight was assigned to the Office of Management and Budget.

Second, for the three cases, EMEA should assess whether the existing data protection standards are implemented in practice and whether there is an effective procedure for individuals to enforce their rights or obtain compensation if things go wrong.

Third, for the three cases, in assessing the circumstances of the transfer, EMEA should take into account, for example, if directly identifiable information is transferred, the security measures to protect the data.

Fourth, it should also take into account the commitments made by the parties (sender and recipient) to keep the information confidential. Also relevant is the commitment not to transfer the data except with prior consultation from EMEA.

Reliance on the exceptions or in contractual clauses: If EMEA does not make use of the possibility to carry out an assessment as described above or if it reaches the views that the data transfers do not provide an adequate level of protection, EMEA may still rely on exceptions to the prohibition set forth under Article 9.6 of Regulation (EC) 45/2001 or adduce adequate safeguards through contractual clauses to be concluded with each of the recipients (ex Article 9.7 of the Regulation).

Of the various exceptions that Article 9.6 foresees, EMEA may be able to rely on 9.6 (d) "*the transfer is necessary on important public interest grounds*". It may be argued that the overall purpose of the transfers of information is to contribute to the protection and reinforcement of public health and thus qualify as a "public interest ground" *ex* Article 9.6 (d). This exception, which is also foreseen in the Data Protection Directive, is meant to apply to data transfers between public administrations, for example in cases of transfer of data between custom, tax, or social security administrations. The case in point qualifies as a transfer between administrations which may be considered as necessary for a public interests ground, in this case, the protection of citizens' health. The interest is not a simple one but rather substantial, which enhances the prospect of applying it.

However, as stated by the Article 29 Working Party, exceptions to the obligation are meant to be applied to occasional data transfers: "*The Working Party would recommend that transfers of personal data which might be qualified as repeated, mass or structural should, where possible, and precisely because of these characteristics of importance, be carried out within a specific legal framework (i.e. contracts or binding corporate rules").*

If EMEA's personal data transfers are sporadic, for example, if they are carried out in very specific cases where the transfer of personal is absolutely necessary, then EMEA may be in a position to rely on this exception. On the contrary, if the data transfers are structural, then, EMEA may have to enter into contractual arrangements, as further explained below, for the purposes of providing safeguards.

On the possibility to use contractual arrangements for the purposes of providing safeguards, the EDPS notes that EMEA has exchanged letters with the three Ministries in Japan, Canada and the United States. There is a question as to whether these letters offer the necessary safeguards pursuant to Article 9.7. The EDPS notes that the letters do not contain specific data protection provisions. They do contain provisions on confidentiality which require keeping the information confidential. They also include a commitment not to transfer the data except with prior consultation from the originator. The content of the exchange of letters does not foresee the application of key data protection principles, such as data quality, transparency, right of access, rectification and opposition or security which are necessary to ensure an adequate level of

protection.

In sum, EMEA may rely on the exception of Article 9.6 (d) if the data transfers are irregular and infrequent. Otherwise, EMEA must decide, in the light of the circumstances of the transfer, whether the recipient provides adequate safeguards for the transfer in question. In case of a negative conclusion, EMEA must enter into contractual arrangements with the three recipients in order to provide adequate safeguards. The EDPS calls upon EMEA to analyse the above options and, in the light of the circumstances of the case in point, work towards compliance. The EDPS wishes to be informed of the outcome of EMEA's analysis. If the selected option is to use contractual clauses, for example, on the basis of the existent exchanges of letters or amended versions, the EDPS urges EMEA to work towards including the key data protection principles and to be notified accordingly.

2.2.8. Information to the data subject

Pursuant to Article 11 of Regulation (EC) No 45/2001, those who collect personal data are required to inform individuals that their data are being collected and processed. Article 12 refers to those cases where information has not been supplied by the data subject. Pursuant to both articles, individuals are further entitled to be informed of, *inter alia,* the purposes of the processing, the recipients of the data, etc.

Pursuant to Article 12.2 of Regulation (EC) No 45/2001, information is not necessary, among others, if (i) the individual already has it or (ii) if the provision of such information proves impossible or would involve a disproportionate effort.

The EDPS has been informed that EMEA does not give any notification to individuals because EMEA has not direct contact with individuals and it would be very cumbersome for EMEA to identify each of these individuals, their respective addresses and give them the requested information. EMEA notes that NCAs, MAHs and sponsors have to comply with national provisions implementing the Data Protection Directive, which require informing individuals of the processing operations and the intended data transfer.

The EDPS agrees with EMEA that in most cases it would be very cumbersome, if not impossible, for EMEA to identify the individuals referred to in ICSRs in order to provide them with the notification. In this regard, the EDPS considers that EMEA, on the basis of Article 12.2 of the Regulation, can argue that it would involve a disproportionate effort to find out the contact details of individuals in order to send them a notification.

However, entities at local level, NCAs and MAHs, can and must provide notification to individuals. In this context, the EDPS considers that EMEA, insofar as it is a joint controller, shares certain responsibility toward ensuring that NCAs and MAHs fulfil this obligation at local level. This is because compliance at local level may, at the same time, ensure compliance at EMEA level. For example, if information at local level includes information about the transfer to EMEA and subsequent use in EudraVigilance, with one information notice, individuals will be informed in compliance with both Member State and EU data protection legislation.

Although EMEA can not police such entities to carry out there obligations in their behalf, it can contribute to facilitate compliance at local level. The EDPS considers that certain actions could be carried out towards this goal. EMEA should enter into a dialogue, at least with NCAs. In the context of this dialogue, it should be discussed how to ensure compliance with this obligation. In this context, the EDPS suggests drafting a notification template, to be used when information is collected at local level. All NCAs should use the template after adapting it at local level. The notification should make reference to the transfer to EMEA and to the dissemination of the information through EudraVigilance.

As a part of their efforts to ensure that notification has been provided to patients, EMEA should consider inserting a warning in the EMEA web site, in the section dedicated to EudraVigilance, and also as a part of the system for NCAs and MAHs when they send their ICSRs to EMEA.

The EDPS calls upon EMEA to engage in such efforts with NCAs and, if possible, with MAHs, in order to ensure that notification to individuals is provided.

2.2.9. 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, at any time within three months from the receipt of the request and free of charge, from the controller, communication in an intelligible form of the data undergoing 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.

The Notification does not refer to the data subjects' rights *of access and rectification* and the procedures to exercise them. According to EMEA, this is because EMEA does not have direct contact with the data subjects. EMEA has informed the EDPS that it has never received an access request from individuals.

The EDPS notes that if individuals are not informed about the use of their data in EudraVigilance, obviously they will never contact EMEA to exercise an access request. simply because they are not aware of the data processing. It is also possible that individuals exercise the access request at local level.

The EDPS considers that EMEA should have in place a procedure to provide access to personal data, and rectification of inaccurate or incomplete data, in case of requests from data subjects. If an access request is received from a patient or other individuals from whom EMEA holds data, EMEA has to analyse such request and react accordingly.

The EDPS understands that in certain cases it may be difficult for EMEA to grant access. However, such difficulty does not remove EMEA's general obligation to consider requests and provide access where required. Yet, if for example, in a given case EMEA is not able to identify the personal information of an individual who requests access to his/her personal information, EMEA can lawfully deny access informing the individual of the reasons.

2.2.10. Security measures

According to Articles 22 and 23 of Regulation (EC) No 45/2001, the controller and the processor must 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. These security measures must in particular prevent any unauthorised disclosure or access, accidental or unlawful destruction or accidental loss, or alteration and prevent all other forms of unlawful processing.

The EDPS notes the technical and organisational measures currently adopted by EMEA with regard to EudraVigilance. The EDPS also notices the adoption by EMEA of standards on information security management. Nevertheless, the EDPS recommends that EMEA adopts the following additional measures:

[....]

3. Conclusion

With exception notably of the issues raised in section 2.2.5 as to "data quality" there is no reason to believe that there is a breach of the provisions of Regulation 45/2001 providing the considerations in this Opinion are fully taken into account. As to data quality, a careful analysis and reassessment of current practices is unavoidable. In particular, EMEA should therefore:

- *Endeavour to engage* in an examination of the possibility to minimize the personal data recorded in ICSRs. Namely, together with NCAs and MAHs, endeavour to carry out an analysis of the data that is really needed in ICSRs, in the different levels (local and EMEA), so that the same standards apply throughout the EU, taking into account the data minimisation principle;

- *Endeavour to engage* in an investigation of the possibilities to anonymise or pseudoanonymise personal information. EMEA together with NCAs or MAHs should evaluate the extent to which and how the data included in ICSRs could be anonymised or pseudoanonymised.

- *Ensure* that it has *legal grounds* to process health related data. To this end, ensure that only data strictly "*required for the purpose of preventive medicine*" is upload in EudraVigilance; otherwise, obtain express consent *ex* Article 10.2(a); If consent is used as legal basis *ex* Article 10.2(a), *cooperate* with NCAs and MAHs so as to ensure that they only send to EMEA health data of patients who have previously consented;

- *Consider* whether a limited conservation period would fulfil the purposes sought by the data processing;

- *Engage in an assessment* of the legal grounds for transferring data out of the EU; assess whether the recipient authorities ensure an adequate level of protection *ex* Art. 9.2; or whether, an exception applies *ex* Art. 9.6(d) because of the irregularity of the transfers. Alternatively, consider entering contractual arrangements which include the key data protection principles. *Inform* the EDPS of EMEA's final decision on the above;

- *Engage on a dialogue* with NCAs, MAHs and sponsors in order to draft a standard notification form to provide the required information to individuals, which should include a reference EudraVigilance. Also, insert an information notice in EMEA web site;

- Put in place a procedure to provide access and rectification of personal data;

- Adopt the security measures described in this Opinion.

Done at Brussels, 7 September 2009

(signed)

Peter HUSTINX
European Data Protection Supervisor