Prior checking opinion on the European Surveillance System ("TESSy") notified by the European Centre for Disease Prevention and Control ("ECDC") on 22 July 2009

Brussels, 3 September 2010 (case 2009-0474)

1. Proceedings

On 22 July 2009 ECDC notified the European Data Protection Supervisor ("**EDPS**") of the European Surveillance System for epidemiological surveillance and control of communicable diseases for "ex-post" prior checking. On 17 July 2009 (upon receipt of an advance copy of the notification via email on 16 July 2009), the EDPS requested a telephone conference to clarify some of the facts. The telephone conference took place on 10 September 2009. During the call ECDC undertook to provide further information. This was provided on 14 October 2009 and 31 March 2010. On 26 May 2010 the EDPS sent the ECDC a summary of his understanding of the facts, including his remaining requests for clarification. The ECDC confirmed the facts and responded to the questions on 17 June 2010. On 18 June 2010 the EDPS extended the deadline to issue his opinion by one month. On 14 July 2010, the EDPS sent the ECDC the draft opinion, for comments. The ECDC commented on 21 August 2010.

2. The facts

2.1. Introduction. This prior checking covers the data protection aspects of TESSy. TESSy is a communication tool used by the European Centre for Disease Prevention and Control ("**ECDC**") and EU Member States for the exchange of information for the prevention of "communicable diseases" which are "relevant at Community level" such as tuberculosis, measles, SARS, H1N1 and others[1]. In particular, TESSy is designed to ensure a rapid and effective exchange of epidemiological surveillance data among EU Member States. As such, it constitutes an important tool to protect public health.

2.2. Personal data exchanged. The personal data are uploaded onto TESSy by contact points (competent health authorities) in Member States. TESSy users mostly rely on pre-defined data fields. Free-text fields are less frequently used (only on an *ad hoc* basis when the pre-defined data fields do not provide for an important piece of information). The pre-defined data-fields may include, typically, the types of diseases, the ages of the patients, their gender, the country of notification and birth, nationality. A large number of other data fields are also used, often depending on the type of disease or other circumstances. For example, sexual orientation is noted in case of sexually transmitted diseases. There are also data fields for information such as "first positive HIV test", "date of diagnosis", "date of death" or "suspected main mode of transmission".

[1] For definitions and further details, please see the documents referenced in Section 2.3 when discussing the legal basis of TESSy.

There are two types of personal data exchanged via TESSy: aggregate data with no "recordID" and "case-based data" with a "recordID".

Aggregate data describes, for example, the total number of cases in a specific country and the proportion of cases with certain characteristics (number of cases in age group 0-5 years, number of cases with male gender, etc.). Case-based data is a set of data referring to a single patient and a single occurrence of a disease. For example one person that has an infection of legionnaire's disease. In cases where it is possible to get an infection multiple times during a patient's lifetime, these episodes are seen as different cases. Examples of case-based data: age, gender, date of diagnosis, date of notification, outcome (dead or alive).

The "recordID" is a number allocated by the uploading party to a set of data relating to a single case (such as one patient with tuberculosis at a specific time, as well as its subsequent follow-up). Its functionality is to allow the uploading party to update the data easily when necessary (for example, to record the patient's subsequent treatment details or recovery). The "recordID" is only accessible to the competent authorities in Member States, and the ECDC. Thus, it is not accessible to other recipients, for example, to the Commission or to the WHO regional office in Europe.

In both cases, "anonymization techniques" are used to protect privacy, remove direct identifiers, and make the indirect identification of the data subjects as difficult as possible under the circumstances. In essence, these techniques are there to strip personal data of personal identifiers (not just direct ones) in order to eliminate or reduce privacy concerns, while still retaining useful information.

As a first step, obvious personal identifiers such as ID numbers, names, dates of birth, etc are routinely eliminated. The techniques, however, often go much further, making it increasingly more difficult to even indirectly identify specific individuals.

With that said, despite use of the "anonymization techniques", and while the purpose of TESSy is not to exchange personally identifiable information, the ECDC explained that sometimes it is necessary to keep data fairly "granular", rather than remaining at a "higher level of aggregation" to ensure that the data will be helpful for the surveillance purposes they are destined for. This is why, for example, case-based data are needed. The need for granularity also explains, for example, why age in months (rather than in years) is needed for vaccine preventable diseases under the age of two.

"Anonymization techniques" are used by the Member States before sending the data to TESSy (unless this is not necessary due to the low risk of indirect identification of data subjects). With that said, there are some personal identifiers left in the database even after use of the "anonymization techniques", which may lead to indirect identification. These include, typically, the following:

- recordId (see description above)
- age
- gender

For certain diseases additional possible identifying information can be retained. This may include, for example:

- date of death
- age in months (only for vaccine preventable diseases and children under age of two)

- country of birth/nationality of patient
- country of birth/nationality of mother of patient (for diseases where mother to child transmission is possible)
- place of residence (in NUTS code regions).

2.3. Legal basis. TESSy is established pursuant to Decision No 2119/98/EC of the European Parliament and of the Council of 24 September 1998 setting up a network for the epidemiological surveillance and control of communicable diseases in the Community ("**Community Network Decision**"). Subsequently, on 21 April 2004 Regulation (EC) No 851/2004 of the European Parliament and of the Council established a separate entity, ECDC, as an independent European centre for disease prevention and control ("**ECDC Regulation**"). The ECDC Regulation designated, in its Article 5.2, the ECDC to operate TESSy.

2.4. The roles of the ECDC and contact points in Member States. The notification indicates the ECDC as the controller of the system. The notification also mentions that the system is "operated by" the ECDC. The Community Network Decision or the ECDC Regulation does not specifically assign the role of "controllers" or "co-controllers" to the ECDC and to Member State authorities or define the role of the Commission in this respect. Neither do they explicitly define the precise roles of the controllers and the involvement or role of any eventual processors.

With that said, it is the understanding of the ECDC that each Member State authority has certain responsibility with respect to its own use of TESSy, and for the data it uploads onto the system, and in that sense, acts as separate controller of the system. At the same time, the ECDC, which operates TESSy and ensures the security of the data exchanged in it, is also considered as a controller, with respect to those activities for which it is responsible, including the functioning and security of the system.

The ECDC further explained that ECDC is not part of the "EU network"; therefore, although ECDC operates the system, and has read access to any data in TESSy, it has no write access and cannot upload data on TESSy.[2] With regard to the Commission, the ECDC is of the view that the Commission (DG SANCO) does not act any more in the capacity of a "controller" as any of the other potential "read-only" recipients listed in Section 2.5 below (for example, the WHO regional office in Europe or EFSA). In particular, the Commission has no write access and cannot upload data on TESSy. Unlike the ECDC, the Commission is also not responsible for the "operation" of the system.

2.5. Recipients. Currently there are over a thousand users in the various competent authorities in Member States with direct access to TESSy.

In addition to competent authorities in Member States, the ECDC, the Commission (DG SANCO), as well as WHO also each can get direct access to TESSy. As for the WHO, the data is accessible to the WHO regional office for Europe, which treats it confidentially, under the International Health Regulations. Thus, the ECDC explained to the EDPS that no data are sent on to individual WHO member states.[3] Other EU agencies (such as EFSA) as well as DG JRC can also get direct access to the data provided that they also treat the data confidentially. Access to

[2] This is with the exception of changes that are made by the operators of the database in response to direct instructions from the Member States (which are logged). These particularly consist of corrections of data that were incorrectly stored in TESSy by the Member State and that cannot be easily corrected by the Member States themselves.

[3] This is with the exception of the HIV/AIDS data which is collected as a "joint surveillance" activity of ECDC and WHO regional office for Europe, where the data are available for all participants of the WHO Euro region HIV/AIDS network.

TESSy may be direct in this case, and granted in a similar manner as to competent authorities in Member States. A contract will be concluded and the persons getting access will have to sign confidentiality agreements. Publication of data is always subject to approval by the Member State that provided the data.

The contact points in Member States can each have both read and write access, that is, they can both upload and view data posted on TESSy. On the other hand, the ECDC, the Commission (including DG JRC), EU agencies and the WHO have only read access. They cannot post or modify data in TESSy.

2.6. Data transfers to third parties. Data requests from academic institutions, universities, non-EU public health agencies, non-governmental organisations and commercial companies will be assessed by ECDC and be subject to "peer review" by a group of three national surveillance coordinators and two ECDC experts according to criteria that ECDC plans to publish on its website. The data will be made available as an extraction from TESSy, and upon signing a contract that defines the rights and obligations of users of TESSy data.

2.7. Information to data subjects. The notification suggests that - considering the fact that personal data are collected at national level and uploaded without an identifier (apart from the recordID) - it is impossible for ECDC to provide data subjects the information contained in Article 12 of the Data Protection Regulation.

2.8. Access rights (including rectification, erasure and blocking). For the same reason, ECDC explained that it is impossible for ECDC to provide data subjects with the right to access, rectify, block, erase or object to the use of personal data.

2.9. Retention period. The Notification explains that considering the "anonymous" nature of the data, data are kept indefinitely. ECDC further explained that the analysis of the data is always done in retrospect in cases where proper statistical analysis (especially concerning correlations) can only be done using the most granular data available.

2.10. Security measures. ECDC explained that a policy on data submission, access and use of data within TESSy has been approved by the management board of ECDC. This policy details the different user's access rights and responsibilities. According to the document provided to the EDPS, this policy will be confirmed and signed by all Members States and the Commission "after the review in 2010".

When requested to provide a copy of the security policy relevant to TESSy, ECDC further explained that a system-specific security policy will be developed, along with a general information security policy, by the ICT Security Officer recently recruited by ECDC.

3. Legal aspects and Recommendations

3.1. Applicability of the Regulation. The notified processing, insofar as it concerns the activities of the Commission and the ECDC, falls under the scope of Regulation (EC) 45/2001 ("**Regulation**") pursuant to its Articles 2 and 3. The processing of personal data by the Commission and ECDC is supervised by the EDPS (see Regulation, Article 1).[4]

[4] For a national contact point in a Member State the applicable law is its own national data protection law which must be in conformity with Directive 95/46/EC. The processing of personal data by these contact points is supervised by their national data protection authorities.

It is important to note that statistical data in certain situations may constitute personal data despite the fact that various "anonymization techniques" are used, following standards common in the field of statistics. As the EDPS previously analysed in consultative opinions[5], "*although, from a data protection view, the notion of anonymity would cover data that are no longer identifiable, from a statistical point of view, anonymous data are data for which no direct identification is possible. This definition implies that indirect identification of data would still qualify these data as anonymous, from a statistical point of view*".

The first step is usually the removal of direct and obvious personal identifiers such as ID numbers, names, dates of birth, and so forth. Various other "anonymization techniques" are then also often used to make it increasingly more difficult to identify specific individuals.

Despite these efforts, it must be emphasized that the data will continue to be considered as "personal data", and thus, subject to the Regulation, so long as the individuals can be indirectly identified. The mere fact that "anonymization techniques have been used", does not mean that the data are considered as "anonymized" in the meaning of recital 8 of the Regulation.[6]

It is also important to point out to the status of "key-coded" data. In such cases individuals are "*earmarked by a code, while the key making the correspondence between the code and the common identifiers (like name, date of birth, address) is kept separately*."[7] This may mean that in certain situations using the "codes" the relationship between a statistical data or set of statistical data and an individual data subject can be re-established. This is sometimes specifically intended, such as in a clinical trial situation to allow treatment of patients in case of adverse health effects or in longitudinal studies. Other times the ability to identify individuals is not necessary beyond the initial period which may be necessary to verify the accuracy of the statistics. In any event, adequate technical, organizational and legal measures should be taken to ensure that the codes will only be used when this is specifically intended for a clear and well-defined purpose. So long as the keys are not destroyed and the possibility of re-establishing a direct link to the individual remains, the key-coded personal data cannot be considered fully "anonymous".

Key-coded data have relevance in two aspects in TESSy. First, in case of case-based data, using the recordID, the competent health authority which initially uploaded the data will be able to identify the individuals concerned. Second, even in cases where aggregate data rather than case-based data are uploaded to TESSy it may still be possible, at least in some cases, that the competent authorities in Member States or others (for example, those who initially collected the data) still hold the keys that would enable them to identify the individuals concerned.

3.2. Grounds for prior checking. The processing is subject to Article 27(2)(a) of the Regulation which requires prior checking by the EDPS of, among others, "processing of data relating to health".

3.3. Deadlines for notification and for issue of the EDPS opinion. TESSy was already in use before the EDPS was notified, and therefore, this prior checking procedure is now carried out and the EDPS recommendations need to be implemented ex post. For the future, the EDPS calls

[5] See Opinion of the European Data Protection Supervisor on the proposal for a Regulation of the European Parliament and of the Council on Community statistics on public health and health and safety at work OJ 2007/C - 295/01, and Opinion of 20 May 2008 on the proposal for a Regulation on European Statistics (COM(2007) 625 final), OJ 2008/C - 308/01

[6] Recital 8, see notably: "*To determine whether a person is identifiable, account should be taken of all the means likely to be reasonably used either by the controller or by any other person to identify the said person*".

[7] See, for example, page 18 and onwards of Opinion 4/2007 of the Article 29 Data Protection Working Party on the concept of personal data.

ECDC's attention to the fact that the opinion of the EDPS should, as a rule, be requested and given prior to the start of any processing of personal data.

Pursuant to Article 27(4) of the Regulation, this opinion must be delivered within two months, discounting any periods of suspension allowed for receipt of additional information requested by the EDPS. The procedure was suspended for 261 days (plus the month of August in 2009 and 2010). Further, the EDPS extended its deadline to issue an opinion by one month. The opinion must therefore be provided no later than 6 September 2010.

3.4. Lawfulness of the processing (Article 5(a) of the Regulation). The processing is based on the legal basis described in Section 2.3 above. Thus, specific legal instruments "adopted on the basis of the Treaties" allow and provide the basic conditions for the notified processing operations. The EDPS is also satisfied that the processing of personal data, after use of adequate "anonymization techniques" (proportionate to the risks to privacy) and subject to other safeguards as provided in this opinion, is necessary and proportionate for the public interests of protecting public health in the European Union. Therefore, the processing is lawful. With that said, it is recommended to strengthen and clarify the legal basis of the processing by establishing a more clear division of tasks and allocating more clearly the responsibilities, in particular, as among the ECDC, the Commission and Member State contact points, as will be described in Section 3.5 below.

3.5. Allocation of responsibility for the operation and use of TESSy. As a preliminary remark, the EDPS emphasises that in any situation where personal data are processed, it is crucial to correctly identify who the controller is. This has recently been emphasized by the Article 29 Data Protection Working Party in its Opinion 1/2010 on the concepts of "controller" and "processor", which was adopted on 16 February 2010. The primary reason why the clear and unambiguous identification of the controller is so crucial is that it determines who shall be responsible for compliance with data protection rules.

As noted in the Working Party Opinion[8], "[i]f it is not sufficiently clear what is required from whom - e.g. no one is responsible or a multitude of possible controllers - there is an obvious risk that too little, if anything, will happen and that the legal provisions will remain ineffective." Clarity is especially needed in situations where multiple actors are involved in a cooperative relationship. This is often the case with EU information systems used for public purposes where the purpose of processing is defined in EU law.

For these reasons, the EDPS urges the Commission and the ECDC, to lay down, in a clear and unambiguous manner, the tasks and responsibilities of each party involved in the data processing, including the ECDC, the Commission and contact points in Member States. Ideally, and in the medium term, this should take a legally binding form, in EU legislation. As an interim solution (but also, to provide further detail in the long term even if further legislation will be adopted), clarifications may be provided in another, more practical form. This may take different forms. One possibility would be to adopt a set of data protection guidelines for TESSy. Technically, this may take, for example, the form of a Commission Recommendation.[9]

When allocating responsibilities in the TESSy data protection guidelines, in particular, the following issues need to be addressed:

- Who are responsible for ensuring the quality (proportionality, accuracy, etc) of the data?

[8] See page 7, Section II.3 of the Opinion.
[9] See, for example, the Commission's Data Protection Guidelines for the Internal Market Information System at http://ec.europa.eu/internal_market/imi-net/docs/recommendation_2009_C2041_en.pdf

- Who can determine retention periods?
- Who determines who can have access to the database?
- Who are authorized to make a transfer of the data to third parties?
- Who are providing notice to data subjects?
- Who are responsible for acting when access, rectification, blocking, or erasure is requested by data subjects?
- Who bears ultimate responsibility for the security of TESSy?
- Who makes decisions regarding the design of TESSy?

With respect to each item, it must be clarified who is authorized to make the ultimate decision, but also, who is making the decisions at the practical level and in what manner. If multiple parties are involved in any aspect, the rules for their cooperation and responsibilities should be clarified.

Controllers and processors must be clearly indicated in a way which corresponds to the effective role as well as the legal status of the institutions and bodies involved.

Finally, considering the number of different parties involved, and while fully acknowledging the role that national data protection authorities may play in ensuring compliance by the national contact points, the guidelines may also serve as a means of promoting best practices and a consistent and transparent approach.

3.6. Data quality (adequacy, relevance, proportionality, fairness, lawfulness, purpose limitation, accuracy: Articles 4(1)(a),(b)(c) and (d)).

In general terms, the EDPS is satisfied with the design of TESSy for purposes of data quality, and has not detected any systemic failures leading to significant quality issues.

With that said, maintaining compliance requires continuous efforts and attention. Each user of the system with write access is individually responsible for the quality of data that they themselves upload. To facilitate compliance by the various users, the EDPS recommends that data protection elements should be integrated to any training given to the users of the system. This may include, among others, information on

- how to ensure that only relevant and not excessive data are included in the database (e.g. appropriate "anonymization techniques" are used),
- how to ensure that any incorrect data are rectified and data included are kept up-to-date,
- how to inform data subjects, and
- how to provide them access to their personal data, upon request.

The existence of TESSy guidelines and the importance of integrating data protection into the training given to the users of the system should be brought to the attention of national contact points. The guidelines should also be prominently displayed in the TESSy user interface, and should, as best practice, contain practical examples.

As a specific issue, the EDPS also reminds ECDC that free-text data fields should be carefully edited to ensure that the level of data protection risks would be similarly low as in the rest of the database - for example, all direct personal identifiers should be removed and no outliers should be present in the data.

3.7. Retention of data (Article (4)(1)(e)). With regard to retention, the EDPS recommends that recordIDs be deleted as soon as they are no longer necessary for purposes of updating the

database. The deletion should be automated, its criteria well defined, and ensured by "building" it into the system architecture.

Apart from the record-ID, the EDPS, at this time, pending further technical and other developments, has no objection against retaining data for an indefinite period of time, provided adequate "anonymization techniques" are used, and further provided that access to them remains limited and secure, as described elsewhere in this opinion.

3.8. Recipients and data transfers. The EDPS welcomes the fact that the scope of the recipients and potential recipients of the data is limited to those identified in Section 2 and that safeguards are proposed to ensure that the data disclosed remain confidential and will only be used for genuine research purposes. In particular, the EDPS welcomes that there is a specific procedure ("**peer review**") established to decide upon access requests according to transparent criteria (which is yet to be determined and published). The EDPS also welcomes that the data will only be made available upon signing a contract that defines the rights and obligations of users of TESSy data.

These safeguards are indeed necessary to ensure the privacy of the data subjects concerned so long as the data disclosed to third parties are not fully "anonymous".

The EDPS emphasises that justification for the necessity of the transfer under Article 8(b) of the Regulation needs to be appropriate. What really matters in the end is that (i) the transfers, as a matter of fact, are made for genuine research purposes and that the researchers (ii) will safeguard the confidentiality of the data and (iii) will only use them for the specified research purposes. The peer review procedure must include, among others, that the applicant third party should specify a research purpose, the peer reviewers check the identity and the credentials of the researcher (e.g. whether he or she is affiliated with a research institute), have him sign a confidentiality undertaking, and ensuring the security of data (e.g. by providing a secure internet connection, or encrypting data which are provided on a media support). It should also be noted that researchers will be subject to their own national law for any processing taking place after transfer, including any provisions on supervision, liability and enforcement. With that said, the EDPS recommends that the contract itself should also include appropriate sanctions for the case where it is found that researchers or organizations have breached the undertakings they made.

In addition, the EDPS reminds the Commission and the ECDC that any international data transfers, in particular, any data transfers to the WHO may only take place subject to Article 9 of the Regulation. The EDPS recommends ECDC to explore the possibilities of compliance with this Article in the framework of the follow-up of this prior checking opinion, with the assistance of their Data Protection Officers ("**DPOs**").

3.9. Right of access and rectification (Article 13). Despite the statistical nature of the data (and even if the possibility of identification is only indirect), the ECDC should re-assess whether there may be any situations in which a data subject may wish to have access to their data, rectify such data, or object to its use. Adequate measures should be put in place to address such situations, even if access requests may be rare. This should be established in the data protection guidelines for TESSy, on DG SANCO's (or ECDC's) website dedicated to TESSy, and should also be made available for the users of the application, from within the TESSy application. At a minimum, a contact person should be indicated at each organization using TESSy to deal with access requests. When allocating responsibilities among the various parties, as suggested in Section 3.5 above, it must be assessed who are best positioned to provide access to the data subjects (for example, the organization that initially uploaded the data may be the only one who is able to link the statistical data to the data subject using a key that it may hold).

3.10. Information to the data subject (Articles 11 and 12). Articles 11 and 12 of the Regulation require that certain information be given to data subjects in order to ensure the transparency of the processing of personal data. Considering that TESSy is used in 30 different countries as well as at the ECDC, the Commission and the WHO contact point for Europe, it is essential that consistent information is made available to data subjects regarding the workings of TESSy, how their data are processed and how they can exercise their rights.

The ECDC, as the operator of the system is best positioned to play a coordinating role and provide centrally and easily available information on-line, on its website.[10] This should be complemented, whenever possible, by data protection notices provided by competent authorities in Member States according to their applicable laws.

3.11. Security measures (Article 22). The EDPS recommends that ECDC should develop a dedicated security policy for TESSy. This policy should be based on an accurate risk assessment which should identify the potential threats to the system and its communication part. This action should identify stringent security measures for implementation or validate those already in place. This security policy should complement the access right policy already defined and should also - among others - clarify the use of the log files of the application, the security of the communication between the users and the system, and the management of the system administrator's access rights.

The procedure for ECDC to modify/correct data at the request of a user in a Member State (which is regarded as an exception for actions that are difficult or impossible to perform by the users in the Member States with the current tools available) also needs to be documented in detail. The EDPS welcomes the fact that this procedure is logged although the ECDC should explore the possibility to altogether avoid this procedure in the future and to provide the Member States with the necessary tools to correct the data themselves in all cases.

Considering the significant number of users (around one thousand) and the interaction between the ECDC and the Member States for managing these users, the EDPS recommends that the ECDC should explore the possibility of implementing a time limit for user accounts. The user nominator should have the possibility to request the creation of a user account and set a limited period of time after which the account would be automatically closed. If accounts with an indefinite period of time are maintained, the ECDC should request on a regular basis the user nominator to review and confirm the list of users. (When commenting on the draft EDPS opinion, ECDC confirmed that it currently takes this latter approach, that is, while the accounts are set for an indefinite period of time, regular reviews are foreseen.)

Conclusion

The EDPS finds no reason to believe that there is a breach of the provisions of the Regulation provided that the recommendations in Section 3 are implemented, namely:

- **Allocation of responsibilities**

  Controllers and processors must be clearly indicated in a way which corresponds to the effective role as well as the legal status of the organizations involved. It must be specified who is responsible for what, and how data subjects can exercise their rights. Adoption of a set of data protection guidelines for TESSy is recommended.

[10] See, for example, http://ec.europa.eu/internal_market/imi-net/data_protection_en.html, which provides information on the data protection aspects of the Internal Market Information System.

- **Data quality and training**

Data quality should be individually assessed by the users uploading personal data on TESSy. To facilitate this, data protection should be integrated into the training provided to users.

- **Retention of data**

Record IDs should be automatically deleted when their use is no longer necessary.

- **Transfers to third parties**

Additional safeguards should be implemented, as discussed in Section 3.8, with respect to transfers to third parties and the WHO.

- **Access rights of data subjects**

Despite the statistical nature of the data, the ECDC should re-assess whether there may be any situations in which a data subject may wish to have access to their data, rectify such data, or object to its use. Adequate measures should be put in place to address such situations, even if access requests may be rare. At a minimum, a contact person should be indicated at each organization using TESSy to deal with access requests.

- **Information to data subjects**

To ensure consistency and transparency, the operator of TESSy should provide comprehensive and user-friendly information to data subjects on its website. This should be complemented by notice provided by Member State contact points in accordance with national data protection laws.

- **Security**

A dedicated security policy should be adopted as soon as possible to help ensure the security of TESSy, and to verify and document good administration. Should the three months provided for follow-up on the recommendations of this opinion be insufficient to ensure the adoption and implementation of such a policy, ECDC, within three months, should report on the measures taken thus far, and provide the EDPS with a clear roadmap (including action items and deadlines) for final adoption and implementation.

Done in Brussels, on 3 September 2010

(**signed**)

Giovanni BUTTARELLI
Assistant European Data Protection Supervisor