COUNCIL OF EUROPE CONSEIL DE L'EUROPE

Strasbourg, 11 October 2011 T-PD (2011)6_en

CONSULTATIVE COMMITTE OF THE CONVENTION FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO AUTOMATIC PROCESSING OF PERSONAL DATA [ETS No. 108]

Compilation of opinions

DG I – Human Rights and Rule of Law

INDEX

I- Opinion of the T-PD members on the draft texts prepared by the Committee of Experts on New Media (MC-NM) on social networking *(Doc T-PD(2011)04FIN_en).*

Introduction

1. The Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS 108) (T-PD) would like to begin by welcoming the work of the Committee of Experts on New Media (MC-NM).

2. The Bureau of the T-PD was asked for its opinion on two draft texts prepared by the MC-NM on social networking services, namely a draft recommendation (document MC-NM (2010)3) and a set of draft guidelines for social networking providers (MC-NM (2010)8).

3. Following an initial exchange of views on these drafts at its 23rd meeting (22-24 March 2010), the Bureau asked its members to send written comments on the texts to the Secretariat to help it with the preparation of its opinion. Draft opinions of the Bureau were prepared and circulated to delegations for possible comments. Considering the importance of the matters concerned, the Bureau decided to amend its proposed draft opinions on the basis of comments received and to submit the new drafts as opinions of the T-PD. The drafts were consequently submitted for final validation and comments to the delegations.

Structure

4. The T-PD would point out firstly that it is not always easy to make the link between the two draft texts (recommendation and guidelines), among other things because the recommendation itself refers to a separate set of appended guidelines.

5. Although it is specified in the guidelines for service providers that they must be "read and understood in connection with … the [draft] recommendation", steps should be taken to ensure that a consistent, exhaustive set of principles are also made available to service providers. For example, the guidelines for service providers do not refer to the indexing of data using external search engines whereas measures enabling users to give their free, specific and informed consent to such indexing, for which systematic and automatic provision must be made, relates first and foremost to service providers. This point could be added after that relating to the automatic limiting of access to data to self-selected "friends"[1]. The same applies to the need to raise awareness and educate users on the necessary consent of third parties where publication of their personal data is at stake : this should concern providers specifically.

References

6. The T-PD draws the MN-CM's attention to the texts already adopted on this subject at European and international level, to which reference should be made, at least in the explanatory memorandum on the recommendation, beginning with Convention 108.

7. Particular mention should be made of Opinion 5/2009 on online social networking, adopted on 12 June 2009 by the Article 29 Data Protection Working Party, the Resolution on Privacy Protection in Social Network Services adopted in Strasbourg on 17 October 2008 by the 30th International Conference of Data Protection and Privacy Commissioners and the report on the subject adopted in Rome on 3 and 4 March 2008 by the International Working Group on Data Protection in Telecommunications (IWGDPT) known as the "Rome Memorandum".

[1] This notion of "friends" does not seem suited to social networks based on professional relationships.

Data protection principles

8. Generally speaking, the word “finalité” rather than “objectif” should be used in the French text when referring to the purpose of processing (the word “purpose” is used throughout the English).

9. With regard to the rights and obligations of the persons concerned, the T-PD would point first and foremost to the need for all users of social networking services to be informed about the processing of their personal data in a clear and understandable manner, in language geared, where necessary, to the target audience. This information should be available in the official language of the various user groups’ countries of residence. It must alert users to the dangers of publishing personal data concerning themselves or a third party and the means at their disposal to restrict access so as to keep certain matters in the private sphere. The information provided must be comprehensive and cover subjects such as the identity of the controller, the purposes of the processing, external parties who could process the data and for which purposes, the maximum length of time for which data may be kept, the existence and means of exercising their rights to access, correct, delete or object (locking), as well as conditions for the indexing of data by search engines.

10. It should be emphasised that the rights that users exercise over their personal data are not limited to data deletion (a definition of the user’s “profile” will have to be given) and that providers must make it simple to carry out the various functions on offer, in particular protection of confidential data, visible and easy to use. The idea of data “portability” and what it implies should figure in the draft texts. User interfaces should be simple to use and enable users to fully understand the impact of their actions on their personal data (making it clear for example that by using a particular application their entire list of contacts will be used to send direct notifications to these contacts – a process that inevitably entails their prior consent). Prior and explicit consent should also be the rule in case of use of facial recognition to tag photos.

11. Non-users of the social network may also have their personal data published by users of the service without their consent and should thus have effective means of exercising their rights, in particular the right to an effective remedy. It should be recalled that users also have obligations in respect of third parties (whether they are themselves users or not) and that, in particular, publication of information related to third parties should respect data protection requirements.

12. The T-PD points out that certain categories of vulnerable people other than children may require enhanced protection systems.

13. The T-PD stresses how much caution is required in the use of age verification systems and suggests that it should be recommended that such systems are made to comply with human rights.

14. With regard to the processing of data by third parties and the service provider’s obligation to “seek the informed consent of users before their data is … processed” (the word “unknowingly” should be deleted as it is not compatible with the effect of informed consent), it should be specified that the user’s decision (refusal or consent) should not have any effect on the continued availability of the service to him or her. There may also be a question as to whether such consent should be obtained before the data are “processed” or before they are forwarded to the third party and whether it is necessary to spell out that the third parties concerned are those “offering the applications”. In this connection, the T-PD draws the MC-

NM's attention to Recommendation (2010)13 on the protection of individuals with regard to automatic processing of personal data in the context of profiling, in which it is noted in the preamble that data processing for the purposes of profiling may relate to data stemming from social networks. In particular, providers should be urged to let users decide themselves what personal data they agree to have processed for advertising purposes.

15. The non-indexability of profiles by search engines should be a default setting and indexation should only be possible if the person concerned has given his or her explicit, free, specific and informed consent.

16. Service providers should respect the principle of "data minimisation", in other words limiting processing only to those data which are strictly needed for the purposes agreed to and for as short a period as possible.

17. Providers should respect the purpose principle. In particular, they should not be allowed to cross personal address books to identify non-users of their service and therefore know their relationships. They should not be allowed to use their users data to develop new services, at least without the explicit, free, specific and informed consent of the concerned subject.

18. Although the call to "apply state of the art security measures" to protect data against unlawful access by third parties is to be welcomed, the T-PD considers preferable to refer instead to the "most appropriate" security measures. In this respect, the T-PD underlines the importance of the principles of "privacy by design" and "privacy by default". Providers should notably be asked to look for technical means strenghtening users' control of their data.

19. In the light of current events, it may be advisable to reiterate under what conditions personal data held by service providers may be forwarded and processed by law enforcement bodies (the police) and what protection mechanisms need to be set up to supervise such use (in particular appropriate garantees such as permission from a judge or a specific authority, see also Recommendation No. R (87) 15 regulating the use of personal data in the police sector).

20. Lastly, provision should be made for the data protection authorities to be called to help set up co- or self-regulatory mechanisms (particularly when drafting instruments such as codes of conduct and reference frameworks).

II- Opinion of the T-PD members on the draft texts prepared by the Committee of Experts on New Media (MC-NM) on search engine providers *(Doc T-PD(2011)05FIN_en).*

Introduction

1. The Bureau of the Consultative Committee of the Convention (CETS No. 108) for the Protection of Individuals with regard to Automatic Processing of Personal Data (T-PD) would first of all like to congratulate the Committee of Experts on New Media (MC-NM) on their work.

2. The T-PD Bureau received a request for an opinion on the two draft texts prepared by the MC-NM on search engines, namely a draft Recommendation (document MC-NM (2010) 4) and draft guidelines for search engine providers (document MC-NM (2010) 9).

3. After an initial exchange of views on these drafts at its 23rd meeting (22-24 March 2010), the Bureau called on its members to send in written comments on the texts with a view to preparing its opinion. Draft opinions of the Bureau were prepared and circulated to delegations for possible

comments. Considering the importance of the matters concerned, the Bureau decided to amend its proposed draft opinions on the basis of comments received and to submit the new drafts as opinions of the T-PD. The drafts were consequently submitted for final validation and comments to the delegations.

Structure

4. The T-PD firstly stresses that the link-up between the two draft texts (Recommendation and Guidelines) is not always easy, particularly because the Recommendation itself refers to guidelines (its appendix).

5. The guidelines for search engines providers do not refer to the Recommendation, even though the latter is supposed to serve as the relevant legal instrument setting out the basic principles guiding the development of national strategies in this field.

6. Conversely, the guidelines for providers comprise a chapter on "the rights of users" which does not appear in the draft Recommendation; such a chapter would seem necessary to clarify individual rights for all concerned.

References

7. The T-PD draws the MC-NM's attention to the relevant texts adopted at the European and international levels, to which their texts should refer, at least in the explanatory memorandum to the recommendation.

8. These texts include Opinion 1/2008 on the data protection aspects of search engines adopted on 4 April 2008 by the "Article 29" Data Protection Working Party, the Resolution on Privacy Protection and Search Engines adopted in London on 2 and 3 November 2006 by the 28th International Data Protection and Privacy Commissioners' Conference, and the joint position adopted on this subject in 1998 and revised in 2006 by the International Working Group on Data Protection in Telecommunications (IWGDPT). Recommendation (2010) 13 on the protection of individuals with regard to automatic processing of personal data in the context of profiling, as well as the revised Directive 2002/58/CE "Privacy and electronic communications", should also be underlined.

Data protection principles

9. Broadly speaking, reference should be made to the "purpose" of data processing rather than the "fin" (in the French version) (the reference in paragraph 7 of the appendix to Recommendation to Article 9 of Convention 108 should in fact be to Article 5 of the Convention), or to the "aims".

10. In the specific case of the purpose pursued, the T-PD notes that the draft texts concentrate on the processing of personal data collected by providers in the context of search requests by a user for the purpose of presenting information available on Internet responding to the search. This is indeed the primary purpose pursued. It should nevertheless be pointed out that the implications in terms of the right to privacy and protection of personal data can be all the more important if search engine providers act as content providers. The aforementioned Opinion 1/2008 points out that by retrieving and combining various types of current information on an individual they can create a new profile, greatly increasing the risk for the data subject than if all the data published on Internet remained separate, and a balance must be achieved between the right to data protection and the right to freedom of expression, the right to information. The purpose of presenting information responding to a user's search (initial purpose, falling within the user's freedom of information) should remain unrelated to the implementation of other purposes by the search engine provider.

11. Providers may store data gathered under search requests on various legitimate grounds (enhance the quality of the service, security, etc). The T-PD underlines that any storage of personal data should be for as a short period as possible and be proportionate to each concerned processing purpose. It should in this respect be recalled that Article 8.2 of the European Convention on Human Rights and Article 9 of Convention 108 foresee precise conditions of derogations and that this proportionality assessment aims at protecting individuals from abusive processing of their personal data.

12. In connection with personal data processing for the purposes of service improvement, the T-PD notes that this should be possible without storing the user's IP address. Another possible purpose is an educational search (for instance, a map of global areas infected by the H1N1 virus was drawn up on the basis of data from search requests); the T-PD stresses that the same result can be achieved by sampling or polling or by anonymising personal data.

13. In the personal data protection field, the concept of "sensitive data" concerns "personal data revealing racial origin, political opinions or religious or other beliefs, as well as personal data concerning health or sexual life, (…) (and) personal data relating to criminal convictions". Data in this specific category cannot be processed automatically unless there are appropriate safeguards (Article 6 of Convention 108). Therefore, when the texts refer to such data (paragraphs 1 and 3 of the guidelines and paragraphs 6 and 7 of the appendix to the Recommendation) to convey the risk of infringement of privacy in the context of processing a large quantity of data, the text might be reworded to stress that the collection and processing of large quantities of data may reveal so-called "sensitive" personal data.

14. The non-indexability of profiles by search engines should be a default setting and should only be possible if the person concerned has given his or her free, specific and informed consent.

15. In connection with the rights of users (which might be the subject of a separate chapter in the appendix to the draft Recommendation, as mentioned above), in addition to the right to access, rectify, delete and object, the T-PD stresses the need for clear and comprehensible general information (which might be set out in a new paragraph 8 in the guidelines). It would also seem necessary to provide users with better training in the facilities at their disposal. The Guidelines for search engines providers could in paragraph 13 on media litteracy also refer to include data protection related matters in the curricula.

16. The T-PD welcomes the draft texts' position on consent, underlining that an explicit consent is preferable to the "opt-out" approach. It should also concern the use of cookies. Consent should in fact also be obtained for any subsequent processing of the data, including the transmission by a search engine of the content of the search made by a user to the website presented by the search engine and to which the user accesses in this way. Point 3 of the Guidelines for seach engines providers could be reformulated in order to better reflect Recommendation (2010) 13 on the protection of individuals with regard to automatic processing of personal data in the context of profiling which provides for a free, specific and informed consent in view of the collection and processing of personal data for profiling purposes.

17. In connection with the right of users to control their personal data, notably by correcting or deleting them (paragraph 8 of the guidelines for providers), a careful balance will have to be struck between various rights at stake. It might also be specified that deletion of data should also extend to data contained in the "cache memory" of the search engines, especially if the data has already been deleted from the original website. Where personal data is made available in that cache, data subjects have the right to request the deletion of possibly excessive and inaccurate data.

18. The user's right to opposition in terms of subsequent data processing should also concern the publication of personal data in the search results ("no robot" instruction). It should be foreseen that the technical "no robot" instruction attached to a page or a document of the website publishing this information be strictly respected by the search engines.

19. Paragraph 8 of the appendix to the draft Recommendation on cross-correlation of data might include a reference to Recommendation (2010) 13 on the protection of individuals with regard to automatic processing of personal data in the context of profiling.

20. It is vital that the graphical presentation of content displayed by a search engine on the user's screen clearly differentiates between the search result and any commercial advertisements.

III- Opinion of the T-PD on the CODEXTER report on false identity information as a challenge to immigration authorities *(Doc T-PD-BUR(2011)03_en).*

1. Following the transmission to the Committee of Ministers by the Committee of Experts on Terrorism (CODEXTER) of its summary and analytical report on the questionnaire on the challenge that false travel and identity documents and information pose to immigration authorities, the Committee of Ministers, at its 1090th meeting (9 July 2010), decided to communicate it to the Consultative Committee (T-PD) of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108) for information and any comments it might wish to make.

2. The Bureau of the T-PD has taken note of this report and decided to make the following observations, recalling the provisions of Convention 108 and its Additional Protocol, as well as those of Recommendation No. R (87) 15 regulating the use of personal data in the police sector.

3. It should first of all be noted that security, however necessary and desirable it might be, must be achieved with respect for the principles of data protection, especially where the data in question are sensitive, or indeed highly sensitive. Security and data protection must therefore coexist.

4. Exceptions provided for in Convention 108 and its Additional protocol may be applied in connection with access to and knowledge of data processing, as strictly required by investigations, with respect for the proportionality principle. No infringement of physical and/or psychological privacy can be justified in breach of the proportionality principle.

5. The Bureau of the T-PD also recalls that an invented identity (an alias) – which is common in surfing on Internet, especially on the social networks – serving solely to avoid using one's real identity in contacts with other users, without preventing the controller from ascertaining the real identity of the person concerned (which means that the police can also ascertain it), cannot be considered criminal or treated as a false identity in such a scenario, and indisputably constitutes a personal data item.

6. In connection with transmitting personal data to third countries, the Bureau of the T-PD stresses that co-operation mechanisms must necessarily be based on a minimum bedrock of rules applicable in the field of personal data protection (Convention 108 and its Additional protocol, as well as other relevant principles such as the Guidelines of the Organisation for Economic Co-operation and Development), and that compliance with these rules must be a sine qua non for co-operation. Derogations from the data protection principles can only occur in the strict framework of

the exceptions provided for by Convention 108 (e.g. national defence requirements) and respect for the proportionality principle must be complete.

7. Procedures to assess the level of data protection proper destinations for personal data that reflect the specifics of criminal cooperation could be considered. Harmonisation of national legislations might be useful, particularly in connection with Internet, with a view to securing a minimum number of common concepts.

8. The use of investigatory resources and tools (e.g. identification algorithms) should not be prevented, provided that they respect data protection principles.

9. The Bureau of the T-PD advocates reinforcing co-operation with CODEXTER. The fight against terrorism and organised crime poses difficult challenges which, in the spirit of uncompromising respect for human rights, must be conducted in a spirit of teamwork, with respect for difference and the complementarity of all contributions.

IV- Opinion of the T-PD on Recommendation 1960(2011) of the Council of Europe's Parliamentary Assembly on the need for a global consideration of the human rights implications of biometrics *(Doc T-PD-BUR(2011)13_en).*

1. Following the adoption by the Standing Committee of the Parliamentary Assembly (11 March 2011) of Recommendation 1960(2011) - " The need for a global consideration of the human rights implications of biometrics ", the Committee of Ministers decided to convey this Recommendation to the Consultative Committee of the Convention for the protection of individuals with regard to the automatic processing of personal data (T-PD) for information and possible comments by 30 June 2011.

2. The T-PD Bureau took note of this Parliamentary Assembly Recommendation and decided to make the following comments.

3. The T-PD Bureau firstly wishes to highlight the modernisation work currently taking place on the Convention for the protection of individuals with regard to automatic processing of personal data. In March 2010 the Ministers' Deputies endorsed this important work, one of whose main objectives is precisely that of examining the impact of new technologies on the protection of personal data.

4. The implications of biometrics are thus naturally covered by the current work of the T-PD and will be dealt with in the framework of the modernisation of Convention 108.

5. It should for instance be noted that the consultation document which was published on the occasion of Data Protection Day (28 January) and was intended to allow all key players in data protection to present their opinions on what the modernisation exercise should include, made explicit reference to biometric data, in its question 11 on particular categories of data.

6. The T-PD Bureau also wishes to highlight that the future work to be carried out by the Committee includes a review of the Progress Report on the implementation of Convention 108's principles on the collection and processing of biometric data, (the Progress Report dates from 2005), and a review of Recommendation (97) 5 on the protection of medical data.

7. Finally, it should be noted that the Committee also takes the implications of biometrics into consideration in its current work on the revision of Recommendation (89) 2 on the protection of personal data used for employment purposes.

V- Opinion on Uruguay's request to be invited to accede to Convention 108 and its additional Protocole *(Doc T-PD-BUR(2011)08_en).*

Introduction

On 31 March 2011, the Secretary General of the Council of Europe has received a letter from the Minister of Foreign Affairs of Uruguay requesting that Uruguay be invited to accede to Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS 108, hereafter 'Convention 108'), and to its additional Protocol (CETS 181).

The 43 delegations of the Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (T-PD) have been invited on 8 April 2011 to indicate by 9 May 2011, if they considered that Uruguay had, in accordance with Article 4.1 of Convention 108, taken the necessary measures in its domestic law to give effect to the basic data protection principles of the Convention. Delegations received a copy of the relevant legislation which was appended to the above mentioned request.

A total of 14 positive replies[2] confirming that Uruguay has taken the necessary measures in its domestic law to give effect to the basic data protection principles of Convention 108 have been received by the Secretariat. No delegation objected. The T-PD thus adopted the following opinion through written procedure.

The T-PD recalls that, in 2008, it invited the Committee of Ministers to take note of its recommendation to allow non-member States with data protection legislation in accordance with Convention 108 to accede to this Convention. The Ministers' Deputies took note of this recommendation and agreed to examine any accession request in light of this recommendation (1031st meeting - 2 July 2008[3]).

The T-PD finally wishes to underline that, on 12 October 2010, the Article 29 Data Protection Working Party adopted a favourable Opinion on the level of protection of personal data in Uruguay in the framework of the adequacy procedure carried out by the European Union.

[2] Bosnia and Herzegovina, Cyprus, the Czech Republic, Estonia, Finland, Hungary, Italy, Latvia, "the former Yugoslav Republic of Macedonia", Monaco, Slovenia, Sweden, Switzerland and the United Kingdom.
[3] https://wcd.coe.int/wcd/ViewDoc.jsp?Ref=CM/Del/Dec(2008)1031&Language=lanEnglish&Ver=original&Site=CM&BackColorInternet=9999CC&BackColorIntranet=FFBB55&BackColorLogged=FFAC75

Opinion

In accordance with Article 4 of Convention 108, each Party shall take the necessary measures in its domestic law to give effect to the basic principles for data protection set out in the Convention (Chapter II), including its additional Protocol.

The T-PD notes the following:

- Article 72 of the Constitution of the Republic of Uruguay guarantees the fundamental right to the protection of personal data;

- scope of the data protection regime (Articles 1 and 3 of Convention 108): Uruguay's legislation has a comprehensive scope which covers all types of data processing concerning natural persons performed in the public and private sectors, with the exception of those carried out for strictly personal or domestic purposes, together with that of files governed by specific legislation (sectoral data protection provisions) and the derogations constituting a necessary measure in a democratic society in the interests stated in Article 9 of Convention 108 (see below);

- quality of data (Article 5 of Convention 108): Uruguay's legislation gives effect to the fundamental principles of data protection such as limitation of purposes, quality, lawfulness and good faith, proportionality, accuracy of data and limited time of the retention (cf. Articles 5-8 of the Law);

- special categories of data (Article 6 of Convention 108): Uruguay's legislation provides appropriate safeguards for complementary protection measures for the processing of sensitive data (cf. Articles 18-22 of the Law);

- data security (Article 7 of Convention 108): Uruguay's legislation provides for appropriate measures to be taken for protection against accidental or unauthorised destruction or accidental loss of data (cf. Articles 10-11 of the Law; Article 7 and following. of Decree No. 414/009);

- principle of transparency (Articles 5a and 8a of Convention 108): Uruguay's legislation lays down a general obligation to inform the subject of personal data processing (cf. Articles 13 & 9 of the Law; Article 5 and following. of Decree No. 414/009);

- additional safeguards for the data subject (Article 8b to 8d of Convention 108): Uruguay's legislation provides for and implements the rights of access, rectification (deletion where appropriate), including the right of objection and the right of the data subject to take legal action (cf. Articles 14-17 & 37-45 of the Law; Articles 9-14 of Decree No. 414/009);

- exceptions and restrictions (Article 9 of Convention 108): Uruguay's legislation provides for exceptions and restrictions to the basic principles of data protection which are confined to what is necessary in a democratic society (cf. Article 26 of the Law);

- sanctions and remedies (Article 10 of Convention 108): Uruguay's legislation provides effective procedural mechanisms: in particular, deterrent sanctions (cf. Article 35 of the Law; Article 32 of Decree No. 414/009) and rights of appeal, speedy judicial procedures without charge for any subject of personal data processing (Articles 9, 14-17 and 37-45 of the Law; Articles 10-14 and 29-30 of Decree No. 414/009);

- transborder data flows (Article 12 of Convention 108 and Article 2 of its additional Protocol): Uruguay's legislation contains specific provisions governing transborder data flows of a personal nature, proscribing in particular the transfer of personal data to states or international organisations not ensuring an adequate standard of protection consistent with the rules of international law or of regional legislation (cf. Article 23 of the Law; Articles 4 and 34-35 of Decree No. 414/009);

- supervisory authorities (Article 1 of the additional Protocol): Uruguay's legislation provides for a supervisory authority for data protection, holding real functions of advice, information and supervision together with effective powers of investigation, intervention (including coercive measures) and court action (cf. Articles 34-35 of the Law; Articles 23-27 & 31 of Decree No. 414/009).

In light of the above, the T-PD considers that Uruguay has taken the necessary measures in its domestic law to give effect to the basic data protection principles of Convention 108 and of its additional Protocol. Consequently it supports its accession to the Convention and to its additional Protocol, pursuant to Article 23 of Convention 108.

VI - Revision of the OECD Guidelines governing the protection of privacy and transborder flows of personal data *(Doc T-PD-BUR(2011)14 _fr).*

1. The Bureau of the Consultative Committee of the Convention for the protection of individuals with regard to automatic processing of personal data [STE n°108] welcomes the initiative of the Organisation for Economic Co-operation and Development to review its Guidelines governing the protection of privacy and transborder flows of personal data.

2. The Bureau wishes to emphasise that these guidelines remain fully relevant more than 30 years after their adoption due to their general and technology-neutral approach.

3. The Bureau also stresses that work on updating and reviewing Convention 108 and its Protocol is currently underway in the Council of Europe.

4. The Bureau recalls that the two texts (OECD Guidelines and Convention 108) were developed at the same time and in a coordinated and concerted way, and that the consistency and convergence of these two texts must be preserved.

5. Indeed, such convergence ensures a similar and harmonised level of data protection and promotes the free flow of data while guaranteeing a high level of protection for human rights and fundamental freedoms (especially the right to respect for private life) when processing personal data.

6. The Bureau believes that this need for consistency between the various systems (including the legislative framework established in the European Union) could be reflected in a more obvious

way in the draft mandate for the Guidelines' review and it remains at the OECD's disposal for contributing to the review exercise and to the conservation of the current convergence.