

Strasbourg, 23 June / juin 2011

T-PD-BUR(2011) 12 MOS

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

LE BUREAU DU COMITE CONSULTATIF DE LA CONVENTION POUR LA PROTECTION DES PERSONNES A L'EGARD DU TRAITEMENT AUTOMATISE DES DONNES A CARACTERE PERSONNEL [STE n°108]

(T-PD-BUR)

Compilation of comments received from the T-PD members on the draft opinions texts prepared by the Committee of Experts on New Media (MC-NM) on social networking and for search engine providers.

Compilation des commentaires reçus des membres du T-PD sur les projets d'avis préparés par le Comité d'experts sur les nouveaux médias (MC-NM) au sujet des réseaux sociaux et des moteurs de recherche.

> Secretariat document prepared by The Directorate General of Human Rights and Legal Affairs

Document préparé par la Direction Générale des affaires juridiques et des droits de l'Homme

INDEX / TABLE DES MATIERES

BOSNIA AND HERZEGOVINA/ BOSNIE-HERZEGOVINE	3
CYPRUS / CHYPRE	4
ESTONIA / ESTONIE	5
GERMANY / ALLEMAGNE	6
ITALY / ITALIE	9
MAURITIUS (AFAPDP) – MAURICE (AFAPDP)	15
MOLDOVA / MOLDAVIE	16
PORTUGAL	17
SLOVENIA / SLOVENIE	18

BOSNIA AND HERZEGOVINA/ BOSNIE-HERZÉGOVINE

After revision of Draft opinions of the T-PD Bureau on the draft texts prepared by the Committee of Experts on New Media (MC-NM) on social networking and Draft opinions of the T-PD Bureau on the draft texts prepared by the Committee of Experts on New Media (MC-NM) on search engines we inform you that we have no additional comments to add to these texts.

CYPRUS / CHYPRE

Non-Users

In our opinion reference should be made in the text to the need for Social Network Sites to put in place a system whereby non-users can complain to the providers of Social Network Sites in relation to the use of their personal information on such sites.

According to our Data Protection authority (Data Protection Commissioner), non-users are the single biggest category of complainants to the Commissioner's Office in relation to social networks as they often have no means of directing a complaint.

Draft opinions of the T-PD Bureau on the draft texts prepared by the Committee of Experts on New Media (MC-NM) on search engines

Indexing of data

The draft opinion on social networking and the draft opinion on search engines appear to offer alternate views on the indexing of data by search engines.

The draft opinion on social networking provides -

" the indexing of personal data published by search engines should generally be prohibited and made possible only if the person concerned has given his or her free, specific and informed consent"

On the other hand, the draft opinion on search engines provides -

"The Committee of Ministers is convinced of the importance of search engines for the realisation of the value of the Internet for the public and the World Wide Web and considers it important that search engines are allowed to freely index the information that is openly available on the Web."

It is suggested that there should be some reference in the draft recommendation on search engines to the need for consent to the indexing of personal data on social network sites.

Sensitive Data

Reference is made in guideline 6 to "sensitive data". Sensitive data has a specific meaning in data protection legislation. Would it be possible to use an alternative word?

Transparency

Point 3, page 11

We note that point 3, page 11 appears to be at variance with paragraph 3.4 of the Recommendation on profiling (CM/Rec (2010) 13) and Article 5(3) of Directive 2002/58/EC (as inserted by 2009/136/EC) which require the consent of users in the context of profiling and the placing of cookies respectively. The difference in approach requires explanation.

Data Minimisation

Point 9, page 12

In terms of search engines and the proposed maximum data retention period of 6 months we are of the view that a 9 or 12 month retention period is more realistic in terms of what can be achieved by the industry.

ESTONIA / ESTONIE

Estonian Data Protection Inspectorate has no comments on the draft opinions of the T-PD Bureau. The comments made by the Bureau are appropriate and necessary. Thank you for the great job done.

GERMANY / ALLEMAGNE

Draft opinions of the T-PD Bureau on the draft texts prepared by the Committee of Experts on New Media (MC-NM) on social networking and on search engines

Opinion of the Federal Government

In principle, the recommendations by the Committee of Experts on New Media (MC-NM) and the respective opinions of the T-PD-Bureau which have actually tightened up the recommendations in terms of data protection are to be welcomed. Compared to relevant opinions on both issues, both the Article 29 Data Protection Working Party as well as the International Working Group on Data Protection in Telecommunications (IWGDPT, which is also referred to as the "Berlin Group") lag slightly behind the opinions of the MC-NM. Even though the T-PD Bureau refers to these other positions in its opinions, it would be desirable to incorporate a few specific items into the opinion of the T-PD-Bureau:

1. Social networking

Appendix 1, Draft Recommendation, No. 4 ("media literacy"): it is proposed that data protection and informational self-determination be incorporated into school curricula

Appendix 1, Draft Recommendation, Guidelines, III Nr. 9, indent 3 (prior consent of other people): it is not just the Member States but also service providers that should be urged to inform users about their rights to privacy (rights to their own photograph etc.). In addition, limits should be imposed on the unauthorised publication of third-party data. One option could, for instance, be a technical facility that only allows personal data or relevant third party links to be published (for instance, using tagging functions) if the persons in question have given their consent.

Appendix 1, Draft Recommendation, Guidelines, III no. 9, indent 5 (pseudonymous profiles): instead of urging the providers to use pseudonymous profiles, it would be desirable to permit the use of pseudonyms in social networking in accordance with Section 13 subsection of the 6 of the Telemedia Act (Telemediengesetz) (TMG).

Draft Opinions of the T-PD Bureau, No. 17 (security measures):

- It is suggested that it would be worth examining whether the catchphrases "privacy by design" and "privacy by default" could be incorporated into no. 17.

- It is suggested that imposing an obligation on providers to notify users in the event of security incidents be considered (in accordance with EU Commission proposal COM(2007) 698 and the resolution adopted by the 76th Conference of Data Protection Commissioners of the Federal Government and the Federal Länder on 6 and 7 November 2008 in Bonn).

- It is true that imposing a general obligation on providers of social networking services to monitor the content / user-generated content (particularly in the form of "deep-packet-inspection") is not an option and is to be rejected. In this respect, reference should also be made to Article 15 of the E-Commerce Directive (Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market) which rules out any such general obligation being imposed on service providers – against the backdrop of a graduated liability system. However, one option worth considering is making providers liable in the event that personal data of third parties is published unlawfully by users and if the providers fail to remedy the situation once they become aware of it. Yet it depends heavily on each individual case whether the publication of third-party data by users, which is hugely common in social networking in practise, is unlawful because it is not covered by

the freedom of opinion or by statutory regulations and occurs without the data subject's effective consent. Providers should be asked, at the very least, to look for technical possibilities that strengthen users' control over use of their profile data and prevent identity theft.

- Providers should be urged to let users themselves decide what personal data they wish to be used for advertising purposes.

- Providers should be made aware of the fact that they are not permitted to collect data compiled by their users on third parties who are not members of the social network without their consent (Article 29 Working Party, Opinion 5/2009 on the use of social networking, 3.5).

2. Search engines

Appendix 1, Draft Recommendations, Guidelines No. 10, 11 (filtering and blocking): In principle, it is to be welcomed that strict requirements are defined in respect of filter mechanisms and blocking of websites and in respect of blocking and filtering of search results of search engines, even though the nature of the Internet as a particularly free means of communication is highlighted. As a rule, blocking of websites is to be rejected as there are doubts about the effectiveness of such measures. From Germany's perspective, it needs to be established that endeavours should focus primarily on erasing all illegal content from the Internet. This aspect has not been mentioned in any of the guidelines so far.

- **Appendix to the Recommendation, Guidelines,** No. 10: emphasising the importance of the freedom of information and the demand for transparency are to be welcomed. As outlined above, considerations on systematic nationwide blocking or filtering should be viewed with a critical eye. It is suggested that this aspect be mentioned again explicitly in Appendix 2, no. 10.

- The possibility of enabling users to prevent information relating to them from being crawled by search engines on the Internet, for instance, by creating a "no-robots" option for a website should be considered, bearing in mind that search engine providers would need to observe this.

- Search engine providers should enable data subjects to delete cache memories if they involve unlawful content, for instance, or if the content has already been deleted on the original website.

- **Draft Opinions of the TPD Bureau**, No. 12 (data storage): instead of distinguishing between whether the storage of search requests that can be linked to a user should be overcome or maintained, it should be defined as a clear requirement that no data that can be linked to an individual user should be kept stored unless the user has given his explicit, informed consent (Recommendation of the 28th International Conference of Data Protection Commissioners, London, 3 November 2006, also the Common Position on Privacy Protection and Search Engines by the International Working Group on Data Protection in Telecommunications (IWGDPT), Washington, 7 April 2006).

- Draft Opinions of the TPD Bureau, No. 13 could be of interest for the area of data retention. The Federal Government would be grateful if the storage period derived from the European Convention on Human Rights and Convention 108 could be explained.

- No. 17: this issue needs to be highlighted in particular. Generally speaking, explicit consent in the form of an "opt-in" should be authoritative and not just the possibility of an "opt-out".

3. Self-regulation

The Federal Government advocates to put more emphasis on self-regulation also at Council of Europe level. In view of the international character of the Internet, self-regulation by the economic sector which is interlinked in Europe and beyond and in which users and consumers can trust, is important and makes sense. It is true that self-regulation cannot substitute legal standards. But especially in the international context it provides swift and unbureaucratic opportunities for sanctioning competitors whose behavior is detrimental to data protection.

ITALY / ITALIE

Draft opinions of the T-PD Bureau on the draft texts prepared by the Committee of Experts on New Media (MC-NM) on search engines

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.

4. It should be stressed that this opinion has been drawn up by the T-PD Bureau and that, in view of the importance of the issues involved, it might be useful to consult the whole T-PD.

This consultation of T-PD members will take the form of a written consultation based on the present opinion and the draft texts, and the T-PD's position will then be transmitted to the Steering Committee on the Media and New Information Services (CDMC) for its plenary meeting from 14 to 17 June 2011.

Structure

5. The T-PD Bureau 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).

6. The guidelines for 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.

7. 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

8. The T-PD Bureau 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.

9. 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).

Data protection principles

10. 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".

11. In the specific case of the purpose pursued, the T-PD Bureau notes that the draft texts concentrate on the processing of personal data collected by providers in the context of search requests because this is 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

Supprimé : by¶ providers 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.

12. Providers store the data gathered under search requests on the grounds that such data helps them subsequently to provide faster, more specific and more efficient responses to their users' requests. The T-PD Bureau would suggest that if the principle of non-storage of such data prevailed, it might be useful simply to retain "cookies"; however, such retention should not necessarily be a matter for the search engine providers, as the users themselves could install the cookies. If data storage by the providers were to be maintained, the retention period should never exceed that laid down for cases of data storage for security purposes, and the user should in all cases be able at any time to request the deletion of the data stored. 13. The T-PC Bureau feels that the data storage issue is closely linked to defining the purpose of the data processing. Data storage for security reasons can be accepted (subject to meeting the conditions on derogations provided for in Article 8.2 of the European Convention on Human Rights and Article 9 of Convention 108) for a maximum period of three months.

These two paragraphs (13 and 14) are not fully clear. In particular, as regards par. 13, we have doubts about the advisability of referring only to "security" as regards data storage purposes. Moreover, we should take into account that the Internet scenario is characterized by several kinds of cookie aiming at different purposes, and for each of them one should consider a proportionate retention period. We also have some problems in figuring out the case of the user "installing the cookies" (par. 13). For these reasons we would suggest replacing the two paragraphs by a more general principle (like the WP29 did in its opinion): " Retention periods should be minimized and be proportionate to each legitimate purpose put forward by search engines providers. If search engine providers use cookies, their lifetime should be no longer than demonstrably necessary".

14. In connection with personal data processing for the purposes of service improvement, the Bureau 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 Bureau stresses that the same result can be achieved by sampling or polling or by anonymising personal data.

15. 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 quantities of data, the text might be reworded to stress that the collection and processing of large quantities of data may reveal socalled "sensitive" personal data.

16. 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 of access and the right to object, the T-PD Bureau 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.

17. The T-PD Bureau welcomes the draft texts' position on consent, rejecting the "opt-out" approach. Consent should in fact also be obtained for any subsequent processing of the data in question.

18. The user's right to object to subsequent data processing, set out in the "Transparency" section of the guidelines, should also cover publication of personal data in the results of search

Supprimé : ¶

requests. This paragraph may need clarification. In the current formulation, it may suggest that a data subject may obtain from a search engine provider – Google, the removal of his/her personal data published by a web site and reachable by means of the search engine. A similar interpretation would lead to enormous problems since it would allocate liability to an entity –the search engine provider-which in principle is not responsible for the content published by third parties. This is why we would suggest considering the above recommendation only with reference to the cache provided by them that may be still available for longer than the original publication. In short, we would refer to the principle stated by WP29 highlighting that: " when search engine providers provide a cache, in which personal data are being made available for longer than the original publication, they must respect the right of data subjects to have excessive and inaccurate data removed from their cache".

19. 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), it might also be specified that deletion of data should also extend to data contained in the "cache memory".

20. 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.

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

Draft opinions of the T-PD Bureau on the draft texts prepared by the Committee of Experts on New Media (MC-NM) on social networking

Introduction

1. The Bureau of 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.

4. It should be emphasised that this opinion is that of the Bureau of the T-PD alone and that it would be advisable to consult the T-PD as a whole in view of the scope of the issues raised. It is planned to arrange for a written consultation of the members of the T-PD on the basis of this opinion and the draft texts and to forward the T-PD's views to the Steering Committee on Media and New Communication Services (CDMC) in time for its plenary meeting of 14 and 17 June 2011.

Structure

5. The Bureau of 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.

6. 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.

References

7. The Bureau of 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.

8. 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".

Data protection principles

9. 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). Examples should also be given of legitimate and illegitimate processing. *Including such sentence without providing for examples may be not advisable and even risky. We would suggest to delete such sentence*.

10. With regard to the rights of the persons concerned, the Bureau of 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

Mis en forme : Police :11 pt, Italique

Supprimé : given clear and understandable general¶ information available in the official language of the various user groups' countries of residence. It must alert users to the 1 This notion of "friends" does not seem suited to social networks based on professional relationships.

dangers connected with publishing personal data 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, the categories of persons or bodies to whom or to which the personal data may be communicated, and the purposes of doing so, the maximum length of time for which data may be kept, the existence and the means of exercise the user's rights,

and conditions for the indexing of data by search engines. Lastly, it must list all of the applicable legislation relating to these issues. As formulated, such sentence seems to be too wide and runs the risk to encourage a sort of "bureaucratic" information listing a wide number of laws which may not be always useful for the user. 11. 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. The idea of data "portability" and what it implies should figure in the draft. 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).

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

13. The Bureau of 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 Bureau 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.

15. The non-indexibility of profiles by search engines should be a default setting , and made possible only if the person concerned has given his or her free, specific and informed consent. We would suggest to avoid the word ("prohibited").

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 a period as short as possible.

17. Atlhough 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 talk of the "most appropriate" security measures) ...

18. In the light of current events, it may be advisable to reiterate under what conditions personal data held by service providers may be used by law enforcement bodies (the police) and what protection mechanisms need to be set up to supervise such use (Recommendation No. R (87) 15 regulating the use of personal data in the police sector.

19. Lastly, provision should be made for the data protection authorities to be called to help set up co- or

Supprimé : of any kind

Supprimé :
Supprimé : means of exercising access
Supprimé : right
Mis en forme : Police :11 pt, Soulignement
Mis en forme : Police :11 pt, Soulignement

Supprimé : ¶

Mis en forme : Police :11 pt, Soulignement

Supprimé : indexing
Supprimé : personal data
Supprimé : published
Supprimé : generally be prohibited
Supprimé : as short
Supprimé : ⊤
Supprimé : (though it may be preferable to talk instead of the

self-regulatory mechanisms (particularly when drafting instruments such as codes of conduct and reference frameworks).

MAURITIUS (AFAPDP) - MAURICE (AFAPDP)

Je me permets de faire quelques commentaires sur les documents envoyes. Si tel est le cas pour la plupart des utilisateurs de reseaux sociaux de ne pas consulter les pages d'avertissements ou d'informations du site concernant leurs droits, on devrait assumer peut etre de leur meconnaissance ou ignorance de ces droits en question. Donc, si cela aurait ete possible pour les service providers de filtrer et/ ou bloquer dans les cas requis, les informations personnelles y compris les conversations online d'une telle facon que tout contenu nocif ou illegal est automatiquement alerte ou "flagged" aux utilisateurs au cours de leur utilisation pour qu'ils prennent justement conscience qu'une telle utilisation porte prejudice a leur vie privee ou autres droits- ce qui donnerait plus de souplesse aux utilisateurs de determiner leur action a suivre.

MOLDOVA / MOLDAVIE

Folowing the examination of the T-PD Bureau draft opinions on draft texts prepared by the MC-NM I consider that the documents mentioned above contain necessary provisions in order to ensure the respect for privacy in connection with processing of personal data within social networks and search engines.

PORTUGAL

We would like to inform you that we have no observations to communicate regarding the opinions above mentioned.

SLOVENIA / SLOVENIE

We support the T-PD Bureau draft opinion on the texts by MC-NM on search machines without additional comments.