



COUNCIL OF EUROPE CONSEIL DE L'EUROPE

Strasbourg, 23 June / juin 2011

T-PD-BUR(2011) 11 MOS rev

BUREAU OF THE CONSULTATIVE COMMITTEE 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 Bureau on the draft texts prepared by the Committee of Experts on New Media (MC-NM) on social networking and for search engines providers

Compilation des commentaires du Bureau du T-PD sur les projets de textes 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

| | |
|--|-----------|
| SOCIAL NETWORKING / RESEAUX SOCIAUX..... | 3 |
| CZECH REPUBLIC / REPUBLIQUE TCHEQUE..... | 4 |
| FRANCE..... | 5 |
| ITALY / ITALIE..... | 6 |
| PORTUGAL | 7 |
| SPAIN / ESPAGNE..... | 8 |
| | |
| SEARCH ENGINES PROVIDERS / MOTEURS DE RECHERCHE . | 9 |
| CZECH REPUBLIC / REPUBLIQUE TCHEQUE..... | 10 |
| FRANCE..... | 11 |
| ITALY / ITALIE..... | 12 |
| PORTUGAL | 14 |
| SPAIN / ESPAGNE..... | 15 |
| SWITZERLAND / SUISSE | 16 |

SOCIAL NETWORKING / RESEAUX SOCIAUX

CZECH REPUBLIC / REPUBLIQUE TCHEQUE

- Respect applicable privacy regulations, especially limit by default access to self-selected friends, apply state of the art security measures and have legitimate grounds for the processing of personal data for specific purposes, including further processing by third parties and use for behavioral advertising. To involve explicitly e.g.CM/Rec(2010) 13
- Offering age-differentiated access should however be treated carefully, as a best effort based on age input provided by the minors themselves]. Je trouve que la proposition doit être beaucoup plus précise – qu’il ne suffit pas de dire “carefully”

FRANCE

Je rencontre la même difficulté qu'Alessandra sur la coordination entre les deux textes comme nous l'avions dit en séance.

Le résultat est qu'on ne sait pas comment lire les points listés dans le document 2010 003 par rapport à ceux du 2010 008.

Dans le document Guidelines (MC-NM(2010)003 je proposerais de rajouter un principe qui est de veiller à protéger les données personnelles de l'indexation automatique par les moteurs de recherche. C'est là en effet que réside la question la plus délicate et qui nécessite que soit mise en place le plus d'actions de coopération.

Par ailleurs, je proposerais de compléter la partie 1 concernant l'information par les points suivants:

- L'information doit permettre non seulement d'attirer l'attention sur les dangers de rendre publique toute information mais aussi et surtout sur la possibilité de limiter strictement les accès afin de préserver une sphère de la vie privée
- L'information doit être complète et porter sur la durée de conservation des données, les modalités d'exercice des droits d'accès et d'opposition, les conditions d'indexation par les moteurs de recherche et les paramétrages possibles pour permettre les accès par des tiers.
- Le rappel aux textes relatifs à la protection des données personnelles.

Dans le document MC-NM(2010)008: quelques propositions de modifications: qui sont en note directement dans le document.

La liste pourrait être resserrée autour de points principaux (informations, obligations de fournisseurs etc.) pour être plus lisible.

I encounter the same difficulty that Alessandra on coordination between the two texts as we said it at the meeting.

The result is that in document MC-NM (2010) 008 is how shall we read the points listed as " guidelines" in this document in comparison with document (MC-NM (2010) 003?

In the document (MC-NM (2010) 003 I would suggest to add a principle which is to ensure protection of personal data by automatic indexing search engines. It seems to me to be a most delicate question which requires that a strong cooperation in between government and social network providers is to be looked for. I also propose to complete Part 1 for information part the following:

- The information should permit not only to attract attention to the dangers of releasing any information but also and especially on the possibility of the strictly limit access to preserve a sphere of privacy.
- The information must be comprehensive and cover the period of data retention, the procedures for exercising access rights and opposition, conditions for indexing by search engines and settings available to enable the access by third parties.
- The reference to the texts on protection of personal data

In document MC-NM (2010) 008: some proposed changes which are noted directly in the document.

The list could be reorganized around main points (transparency of information, obligations of suppliers etc. ...) in order to make it more "readable"

ITALY / ITALIE

Regarding the Draft recommendation on measures to protect and promote respect for human rights with regard to **social networking services** (MC-NM(2010)003) and the Proposal for draft Guidelines for Social Network Providers (MC-NM(2010)008) we would like to share the following observations:

a) We find that the relationship between the two documents is not completely clear and would probably need a better explanation and coordination between the two. (In terms of readability even the use of the term “Guidelines” in Appendix of the Recommendation (MC-NM (2010)003) and in the Proposal of “Guidelines” for Social Network Providers - MC-NM (2010)008) may be confusing). Moreover, although in the Guidelines for Providers (MC-NM (2010)008) it is stated that the two documents must be read together, we believe that each document should give to the addressees a complete framework of principles: for example in the Guidelines for providers (MC-NM (2010)008) no explicit reference is made to the indexability of data through search engines. The principle that user data should be only be crawled by external search engines if a user has given explicit, prior and informed consent and that non-indexability of profiles by search engines should be a default setting should be explicitly addressed to service providers considering that they are the actors directly in charge to set up the privacy settings.

b) It is highly advisable to consider the documents that have been adopted at both European and international level regarding data protection with reference to social networking, in particular: a) Resolution adopted in Strasbourg on the 17th of October 2008 by the 30th International Conference of Data Protection and Privacy Commissioners; b) Report and Guidance on Privacy in Social Network Services adopted by the International Working Group on Data Protection in Telecommunications on the 4th of March 2008 (so called Rome Memorandum); c) Article 29 Data Protection Working Party - Opinion 5/2009 on online social networking. Such documents may particularly useful in order to complete the catalogue of safeguards listed in both (MC-NM (2010)003) and (MC-NM (2010)008). In particular, we suggest to consider that user information should specifically comprise information also about users’ rights (e.g. to access, correction and deletion) with respect to their own personal data. Clear information should also be given about security risks, and possible consequences of publishing personal data in a profile, as well as about possible legal access by third parties (including also e.g. law enforcement, secret services). Attention should be given to the possibility and the conditions under which profiles may be considered as “open sources”, to the respect of the principle of scope of data processing, and to the growing occurrence of “portability” of data among different social networks. Users should be alerted about the need to consider carefully which personal data – not only related to third parties but also to themselves– they publish in a social network profile. They should be alerted that they may be confronted with any information or pictures at a later stage, e.g. in a job application situation. Moreover, a stronger emphasis should be put on the need that providers offer privacy-friendly default settings for user profile information. Default settings play a key role in protecting user privacy, especially if we consider that usually only a minority of users signing up to a service will make any changes. Such settings should be specifically restrictive when a social network service is directed at minors.

c) Finally, we suggest that all those sections of the documents mentioning the “right to privacy” should also refer to the “right to the protection of personal data”.

PORTUGAL

MC-NM(2010)003 en :

Pages 4 and 5 – Remove the square brackets on all par. 4. However the draft should be reviewed in order to put more emphasis on the protection of children and mentally or otherwise disable people. Also, VERY IMPORTANT, recommend measures in the sense of improving the mechanism of the so called “age verification”. A debate and this is this is important to the T-PD also, should be opened with Service Providers, Administrations, user/consumer associations and parents associations, for instance.

MC-NM(2010)008 en :

Page 2

In paragraph that starts with “It is important for individuals using social networking services (...) (and ends with) “(...) but become available to a large public”; replace: “They also have to understand when the information they post online (...)” by “They also have to understand **THAT** the information they post online (...)”. Because “WHEN” is a mistake. ALL the information posted on-line in this manner become public and is even intended be so (even when the user is not fully aware of possible misuses of that data).

Regarding this paragraph:

- “Inform users in particular about the difference between private and public communication and the possible consequences of unlimited access (in time and geographically) to their profile and communication.”

I would like to leave the following comment: Is private (that is to say encrypted or otherwise protected) communication offered? As rule, no.

SPAIN / ESPAGNE

- **Guidelines for social networking providers:**

- A reference should be included on providing users a simple and efficient way to exercise their data protection rights through online means.
- The document refers to “limit default access to self-selected friends”. We would include, in this paragraph, a specific reference to the need to avoid by default the “indexability” of such information by search engines.

- **Protection of human rights with regard to social networks:**

- We agree that information to users should be provided “every time such a challenge might arise”, but we would add that it should be made available in a simple and clear way, and using plain language, in order to make it easily understandable.
- Age verification systems could be a good way to improve children’s safety in social networking environments. It is true that many of the existing tools, in general terms, are not always compatible with the protection of human rights. But, at the same time, technology evolves at a very fast speed, and an adequate solution may be feasible in future. We would prefer a more positive wording, i.e. encouraging the development of age verification systems fully respectful with human rights.
- Data protection rights are not limited to the deletion of a profile. Again, we would include a reference on the need to provide users a simple and efficient way to exercise their data protection rights through online means.

SEARCH ENGINES PROVIDERS / *MOTEURS DE RECHERCHE*

CZECH REPUBLIC / *REPUBLIQUE TCHEQUE*

Transparency about the use of personal data and the respect of data protection regulation

Cross-correlation of data originating from different services/platforms belonging to the search engine provider may only be performed if consent has been granted by the user for that specific service. The same applies to user profile enrichment exercises. Search engines must clearly inform the users upfront of all intended uses of their data and respect all user rights to readily access, inspect or correct their personal data and be in accordance with Recommendation CM/Rec (2010) 13 of the Committee of Ministers to member states on the protection of individuals with regards to automatic processing of personal data in the context of profiling.

FRANCE

I question the use of the term "**sensitive data**" which has a specific meaning for data protection and which could be misread in those documents.

In fact what is meant is that the amount of data collected infringes privacy, even e if some data taken separately are not "sensitive". I therefore propose that the documents rewrite differently the sentences referring to sensitive data or put it with comas.

In the "guidelines" document 004, I would add one point on **the rights of individuals** as it is done in document 009.

I agree with the general remark by Joao Pedro and José about the need of a general, clear and understandable **information** apart from the one given about the processing itself. I propose to incorporate this point between 7 and 8 of the guidelines.

Je m'interroge sur **l'utilisation du terme ' sensitive data'** qui a un sens précis pour la protection des données ce qui peut être mal lu de ce fait. En fait ce que l'on entend c'est que la quantité des données collectées porte atteinte à la vie privée, même si prises séparément certaines données ne sont pas " sensibles" au sens de la protection des données. Je proposerais donc que les documents reprennent plutôt cette idée que de parler de données sensibles.

Dans la partie " guidelines" du document 004, je rajouterais un point sur **les droits des personnes** comme cela est fait dans le document 009.

Je suis d'accord avec la remarque générale de Joao Pedro sur l'information et la formation. qui rejoint les observations de José sur la nécessité d'une information générale, claire et compréhensible. Je propose d'intégrer ce point entre le 7 et le 8 des guidelines.

ITALY / ITALIE

Regarding the draft recommendation on the protection of human rights with regard to search engines (MC-NM (2010)004) and the Proposal for Guidelines for **search engine providers** (MC-NM(2010)009), again, we would suggest to reconsider the relationship between the two documents to ensure more readable and well coordinated texts.

a) In this case too, it is advisable to refer to the work on data protection and search engines done by the International Working Group on Data Protection in Telecommunications (Common Position on Privacy protection and search engines on 15 April 1998, revised on 6-7 April 2006), the 28th International Data Protection and Privacy Commissioners' Conference (Resolution on Privacy Protection and Search Engines), and the WP29, in particular Opinion 1/2008, that - striking a balance between the legitimate needs of the search engine providers and the protection of the personal data of internet users - addresses, inter alia, the definition of search engines, the kinds of data processed in the provision of search services, the legal framework, purposes/grounds for legitimate processing, the obligation to inform data subjects, and the rights of data subjects.

b) The draft recommendation and the proposal for Guidelines mainly consider the data processing carried out by search engines providers related to search history. However, there are other aspects related to the impact that search engines – in their role as content providers that help to make publications on the internet easily accessible to a worldwide audience - have on the right to privacy and data protection and that may deserve consideration. As the WP 29 (Opinion 1/2008) reminds us, “by retrieving and grouping widespread information of various types about a single person, search engines can create a new picture, with a much higher risk to the data subject than if each item of data posted on the internet remained separate”. Such issue must be tackled by finding a correct balance between the right to private life/data protection on one side and the free flow of information/freedom of expression on the other hand. In this sense, we recall the WP29 position according to which “the right to correct or delete information also applies to some specific cache data held by search engine providers, once these data no longer match the actual contents published on the Web by the controllers of the website(s) publishing this information. In such a situation, upon receiving a request from a data subject, search engine providers must act promptly to remove or correct incomplete or outdated information. The cache can be updated by an automatic instant revisit of the original publication. Search engine providers should offer users the possibility to request removal of such content from their cache, free of charge”.

c) The use of term “sensitive data” does not seem to be appropriate in the sentence “an individual’s search history contains a footprint which may include the person’s interests, relations, intentions and should therefore be treated as sensitive data”. (see page 4 of the Draft recommendation, paragraph 6 and 7, and page 2 of the draft Guidelines, paragraph 1 and 3). We should remind that in accordance with Convention 108 and the Explanatory memorandum, “sensitive data” are the special categories of data protected by Article 6 of Convention 108. On the contrary, we have the feeling that the intention of the sentence(s) mentioning sensitive data/sensitivity of data, is to highlight that search histories raise special concerns since they offer a picture of the individual’s interests, habits etc. (which is of course a sharable opinion). It is definitively possible that from search histories sensitive data emerge. But, in order to avoid an incorrect/confusing use of data protection terminology, one may state that the search histories raise special concerns since they may include the person’s interests, relations, intentions and “**reveal special categories of data protected by Article 6 of Convention 108**”.

d) We would suggest mentioning that search history data can be used for commercial purposes but also eventually requested by law enforcement authorities or national security services.

e) On the Draft recommendation, Page 4, chapter III, par. no. 7: the reference should be to Article 5 of Convention 108 and not to Article 9.

f) Page 4, chapter III, par. no. 8: we are not sure that the expression “user profile enrichment exercises” is clear enough especially in its relationship with the “possible profile created for example for direct marketing purposes” mentioned at page 5, p. 9. In any case, reference should be made to the data subjects’ rights in accordance with Article 8 of Convention 108 which also includes the right to obtain the erasure of data unlawfully processed.

e) Page 7 chapter VI. Media literacy and awareness raising should be developed also with reference to data processing.

PORTUGAL

Some general thoughts about search engines in special, or even about Internet use in general :

First the education of users is essential. Users should be aware of the characteristics of the service being offered to them. Not just the “common, general” awareness but objective information and formation about. Awareness of issues such as: does anyone know or will be able to know what I have searched? Users should also be advised by providers of services, not just of Internet Service Providers, to the fact that malevolent behaviors exist and that, as consequence, at least basic safeguards should be taken by using appropriate software and, or hardware, and by avoiding risky surf behaviors.

The large majority of offers regarding search engines are of a commercial nature, only apparently free to users, given the fact that they are paid by advertising. Also profiles are done, if not regarding a certain user (possible and eventually more common on paid services), certainly regarding each product, service, information, searched for that is transmitted to interested suppliers of such services, products or information, therefore supplying to them, at relatively low cost invaluable business information.

Some search engines services, as for instance IXQUICK claim to offer privacy protection (e.g. <http://us2.ixquick.com/eng/protect-privacy.html>) however is it to be believed that only paid search services who, using cryptography, to protect the identity of searchers will offer reasonably effective privacy protection.

SPAIN / ESPAGNE

- **Guidelines for search engine providers:**

- We agree with the position stressed out in the document with regard to consent: it is clearly preferred over any opt-out strategy, and should be obtained in order to use data for further processing purposes.
- The right to object should be included in the second chapter, both in relation to the use of users' personal data for further purposes and to the removal of personal information that should not appear in the search results. In the latter case, an adequate balance between the exercise of this right and the need to avoid any kind of censorship should be stricken.

- **Protection of human rights with regard to search engines:**

- Although consent has a relevant role in the guidelines, in this document it is not referenced likewise, although in our view it would deserve a similar approach.

SWITZERLAND / SUISSE

Concernant les projets de recommandation « moteur de recherche » « réseaux sociaux », deux observations concernant le document MC.NM (2010) 004 :

- au point 6, premier tiret « favorisant une plus grande transparence », sans remettre en question le principe, nous attirons l'attention que ce principe pourrait être en conflit avec le secret des affaires du fournisseur du moteur de recherche et pourrait être influencé de manière négative la qualité des résultats des recherches.
- Au point 7, nous estimons qu'une durée de conservation de 6 mois est trop élevée et qu'en tous les cas, l'internaute devrait pouvoir demander l'effacement de ses données avant l'échéance.