European Digital Rights (EDRi) Submission

to

The Council of Europe Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data [ETS 108] (T-PD)

Modernisation of Convention 108: New Proposals

T-PD-BUR(2012)01Rev2_en of 27 April 2012

Meryem Marzouki

30 May 2012

Contents

European Digital Rights
Rue Montoyer 39/9, B-1000 Brussels
Tel:+32 (0)2 550 4112
E-Mail: brussels@edri.org, http://www.edri.org

About EDRi

European Digital Rights, EDRi, is a European not for profit, non-governmental digital rights organisation. EDRi was founded in 2002 by 10 organisations (only NGOs may be members) from 7 European countries. Since then EDRi membership has grown consistently. Currently 32 organisations have EDRi membership. They are based in or have offices in 20 different countries in Europe. In addition 27 observers participate in the organisation's mailing lists and activities. We think of Europe in terms of the Council of Europe territory - not strictly its Member States.

EDRi's objectives are to promote, protect and uphold fundamental human rights and freedoms in the digital environment. Examples of such fundamental human rights are the freedom of expression, privacy, data protection and access to knowledge.

To this end, we strive to monitor, report and provide education about threats to civil rights in the field of information and communication technology. Among our recent awareness raising tools are our widely disseminated booklets on the various issues EDRi deals with (available at: http://www.edri.org/papers). Another example is our bi-weekly newsletter, the EDRi-gram, which is in its 10th year of high quality reports on digital rights in Europe.

We conduct policy research and offer the results to the public and to national and international bodies. Recent examples are our contributions to the European Commission's expert groups on RFID and on the Internet of Things, our responses to the European Commission and Council of Europe (CoE) consultations and our work as observers to CoE working groups.

Furthermore, EDRi and its members advocate at a national and international level by actively engaging with bodies such as the European Union, the Council of Europe, the OECD (EDRi was instrumental in CSISAC formation and recognition by OECD), The International Conference of Data Protection and Privacy Commissioners (through The
Public Voice Global Civil Society Coalition, which authored the Madrid Privacy Declaration on "Global Standards for a Global World"), The WIPO and the United Nations as well as organising and participating in a number of conferences and public events.

EDRi also serves as a platform for cooperation and common activities, combining the influence, experience, knowledge, and research of its members. EDRi's activities are primarily driven and carried out by its members' representatives in addition to their national activities. Together EDRi members, observers and friends advocate and inform civil society, industry and the policy sector to uphold fundamental rights such as privacy and freedom of speech in the information society.

European Digital Rights
Rue Montoyer 39/9, B-1000 Brussels
Tel:+32 (0)2 550 4112
E-Mail: brussels@edri.org, http://www.edri.org

Introduction

These comments from European Digital Rights (EDRi) refer to the new proposals for the Modernisation of Convention 108, made by the Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data [ETS N°108] (T-PD) and dated 27 April 2012 (T-PD-BUR(2012)01Rev2_en).

These EDRi comments complement its comments on previous versions of the Modernisation of Convention 108, submitted at the following occasions:

- Organization of a civil society consultation as a special session of the PrivacyCamp.eu, held on 24 January 2012 in Brussels (http://edri.org/Privacy-Camp-EU)
- Presentation by Meryem Marzouki during the 5th International Conference on Computers, Privacy and Data Protection, as a speaker on the Panel "Modernising Convention 108 in the Face of the IT Revolution" (27 January 2012, Brussels ; available at: http://edri.org/files/2012Marzouki-CPDP-CoEConv108.pdf).
- Oral comments made by Meryem Marzouki during her participation to the consultation organized by the Council of Europe on 2 May 2012 in Brussels, and attended by both civil society and business organizations.

EDRi reiterates its support to the overall objectives of the Modernisation process, and expresses its satisfaction that most of its earlier comments have been taken into account in subsequent versions of the proposal. While EDRi generally welcomes this latest draft, some provisions still needs some revision as discussed in the current submission. EDRi notes that a number of the criticised provisions below are additions that only appeared, or re-appeared, in the draft dated 27 April 2012.

Article 2 – Definitions

[§a] The current definition of a personal data rightly relates to the notion of the possible identification of the data subject, directly or indirectly. However, the proposed explanatory report note is likely to weaken this definition, since it will lead to consider an individual as not identifiable in case the identification process requires "unreasonable time or effort". This explanatory note should be more restrictive, since in some cases "unreasonable time or effort" may be worth spending in comparison to the (commercial or non commercial) advantage derived from identification. Such reasonableness should thus be evaluated on a case by case basis, with regards to the interests at stake, i.e. with regards to both the privacy interests of the data subject and the purpose of the identification by the data controller.

European Digital Rights
Rue Montoyer 39/9, B-1000 Brussels
Tel:+32 (0)2 550 4112
E-Mail: brussels@edri.org, http://www.edri.org

Article 3 - Scope

[§1bis] EDRi supports the exclusion of the data processing carried out by an individual in the course of purely personal or household activities, unless the data are made accessible to persons outside of this circle. However, this paragraph should specify that this restriction applies whether the data are made accessible intentionally or unintentionally. Indeed, since this paragraph mainly addresses the case where the individual uses social networks or other cloud-based services in order to process the data, there are situations where these data become accessible beyond the private circle, while this was not the user's intention and even in some cases without his/her knowledge (e.g. through changes of privacy settings by the service).

[§1ter] EDRi considers that this paragraph, which allows any Party to the Convention to apply it to legal persons, should be deleted. First of all, it is beyond the scope of the Convention, which deals with the protection of "individuals". Secondly, this provision contradicts the very notion of "personal" data protection. Furthermore, the paragraph raises major concern with respect to freedom of information and the right to access to documents (where the concerned legal person is a public entity) and with respect to the principles of transparency and accountability that are necessary in a democratic society (where the concerned legal person is a private entity).
Additionally, the proposed EU Regulation on data protection does not include such a provision, and it defines the data subject as a natural person only.
While EDRi understands the concern expressed by some current Parties to the Convention, arguing for compliance with their current national law, the reasons stated above relate to the respect of fundamental rights and fundamental democratic principles, and thus supersede the inconvenience of modifying an existing national law. Such legitimate harmonisation is, after all, the ultimate objective of an international Convention.
Similarly, the argument that such provision already exists in the current version of Convention 108 cannot be considered as really sound in the framework of a modernisation process. As a matter of fact, the provision was already tentatively weakened – though not entirely removed as it should be – in previous draft versions of the modernisation, where the provision was relegated to the explanatory report.

Article 5 – Legitimacy of data processing and quality of data

[§2a] This paragraph introduces a consent regime, where the data subject's consent need to be "free, explicit, specific and informed". This provision calls for particular caution, since these characteristics are highly variable according to the context, and are difficult to assess in practice. What is a "free" consent when it is given by the data subject in order to benefit from a so-called free of charge service? What is an "informed" consent when the data subject accept terms of services through a simple click, in most cases without having even read and understood the contract, and sometimes when defaults settings are modified without notice by the service provider? What is an "explicit" or "specific" consent given when using web2.0 services that process data collected via other services? What really matters here is that the given consent be meaningful.

[§2b] This paragraph provides for lawful conditions of data processing in absence of the data subject's consent. EDRi's opinion is that these conditions should be more restricted than in the currently proposed version. To this end, the "overriding legitimate interest" should be an "overriding public legitimate interest in a democratic society" (in reference to data processing by government agencies). In reference to data processing by private entities, EDRi considers that domestic law should not provide for exceptions to comply with "contractual obligations binding the data subject" without any restriction, and thus suggests binding such exceptions with compliance to the fundamental rights to privacy and personal data protection.

Article 6 – Processing of sensitive data

[§1] EDRi supports the need to consider that some data are, or become, sensitive either by their nature, the way they are used or because their processing presents serious risks to the interests, rights and freedoms of the data subject. However, it seems inappropriately restrictive to identify such cases with pre-established categories of data as it is currently done in this provision. For instance, some biometric data are sensitive by their nature and not simply by the use made of them. Same applies to other categories of data listed under **1(b)**.
EDRi therefore suggests to rewrite paragraph 1 as follows:
"The processing of certain categories of personal data shall be prohibited, whether such data are sensitive by their nature, by the use made of them, or where their processing presents as serious risk to the interests, rights and fundamental freedoms of the data subject, notably a risk of discrimination.
Such sensitive data are: genetic and biometric data; data related to health or sexual life; data related to criminal offences or convictions or security measures; and data revealing, directly or indirectly, racial origin, political opinions or trade-union membership, religious or other beliefs".
[§2] This paragraph provides for an exception on the prohibition of sensitive data processing, "where domestic law provides appropriate safeguards". EDRi's opinion is that such safeguards should be more precisely qualified in order to avoid abuses. EDRi suggests as a minimum to add that in such case the processing be subject to prior authorization from the national Supervisory Authority. This would ensure that the Supervisory Authority has the knowledge of this processing of sensitive data and of its operational conditions, and has the ability to assess its relevance and the respect of appropriate safeguards. The result would be to guarantee the exceptional character of a derogation to the general regime of prohibition of sensitive data processing.
Furthermore, the definition of biometric data envisioned in the explanatory report is not accurate: on the one hand, biometric data not only relate to physical, biological or physiological characteristics of an individual, but also relate behavioural ones (such as dynamic signature, key stroke dynamics, walk patterns, etc.); on the other hand, biometric data not only allow the unique identification of an individual but also his/her authentication.

European Digital Rights
Rue Montoyer 39/9, B-1000 Brussels
Tel:+32 (0)2 550 4112
E-Mail: brussels@edri.org, http://www.edri.org

Article 7 - Data security

[§2] This provision, dealing with data breach notifications, is welcome but currently too weak to actually avoid possible breaches of the fundamental rights and freedoms of the data subject or his interests. In order to overcome this problem without imposing too cumbersome and unnecessary obligations on the controller (especially when the controller is an SME), EDRi suggests to consider a two-level system of data breach notification obligation, so that (i) the Supervisory Authority is notified in any case of data breach and (ii) the data subject is also notified when the data breach presents serious risks for him/her or when the Supervisory Authority decides so. A suggested rewriting of this paragraph could thus be as follows:

"Each Party shall provide that the controller shall notify, without delay:

- *The Supervisory Authorities within the meaning of Article 12bis of this Convention of any violation of data;*
- *The data subject when the violation of data presents a serious risk of interference with his/her fundamental rights and freedoms or with his/her interests*
- *The data subject upon request by the Supervisory Authorities."*

Article 7bis - Transparency of processing

[§2] One of the mention currently intended to be made in the explanatory report (information of measures taken in case of transfers to countries which do not have an adequate system of data protection) should appear in the text of the Convention itself, namely as an exception to paragraph 2 of Article 7bis, which currently provides that the controller is not required to provide information on the data processing when "it proves to be impossible or involves disproportionate efforts". Otherwise, it is likely that Article 7bis(2) would be invoked precisely in contexts of transfers to countries which do not have an adequate system of data protection, thus jeopardizing the very purpose of Article 7bis.

Article 8 - Rights of the data subject

All provisions of Article 8 are currently are entitled only upon the data subject request. There is a need to differentiate in this respect between provisions of paragraphs (a) to (f). EDRi suggests that the differentiation be made on the following bases:

- Some provisions need to be guaranteed even without any explicit request from the data subject. These rights are those provided in:

[§a] which refers to the data subject's right not to be subject to a significant decision based on the ground of a data processing.

[§b] which refers to the data subject's right to object to the processing of his/her personal data. If this right is only entitled upon request, EDRi is concerned that this provision may be formulated in a way that could undermine the data subject's right to refuse consent on his/her data processing and could contradict provisions contained in Article 5.

European Digital Rights
Rue Montoyer 39/9, B-1000 Brussels
Tel:+32 (0)2 550 4112
E-Mail: brussels@edri.org, http://www.edri.org

- Some provisions necessarily require a proactive action from the data subject in the form of a request. These rights are those provided in:

[Old§c] which refers to the data subject's right to rectification or erasure.
[§e] which refers to the data subject's right to remedy.
[§f] which refers to the data subject's right to benefit from the assistance of a Supervisory Authority.

- Some provisions are indeed entitled only upon request in the current version of Convention 108. However, EDRi expects much more from the modernization process than simply a status quo on these issues. The modernization process should lead to improvement and widening of the right to information and access to processed data. One way to achieve this progress for citizen rights should be to ensure that such information is provided to the data subject without the need for his/her request, on a regular and reasonable basis (e.g. once a year), in a systematic manner. This would allow for citizen empowerment, and would entitle the data subject to specifically ask for more information, upon request. Otherwise, one might wonder how the data subject could send a request for information and access to his/her data, when s/he does not even know that these data are processed. Rights needing such improvement are provided in:
[New§c] which refers to the data subject's right to information and access to his/her processed data.
[§d] which refers to the data subject's right to information related to the logic underlying the data processing.

Article 9 - Exceptions and restrictions

[§1a] Among the exceptions to the basic data protection principles, this paragraph now includes again the "prevention" of criminal offences. EDRi is very concerned with this new development in the latest draft, since it relates to intelligence purposes, before any infraction has been committed, and not simply to law enforcement purposes. EDRi thus suggests that this exception should either be removed from the current list, or at the very least be accompanied with adequate additional safeguards.

Article 12bis - Supervisory authorities

[§3] (competent authority). EDRi wonders whether this provision would remain compatible with the EU Regulation, especially given that the Modernization process of Convention 108 will be completed before the adoption of the EU proposed Regulation on Data Protection. This paragraph should thus be written in a neutral way with this respect.
[§9] (lack of competence of Supervisory Authority with respect to data processing by judicial bodies). EDRi fears that this very generic wording could apply not only to a judge, but also to a prosecutor during police investigation. EDRi thus suggests to clarify the wordings of this paragraph.

European Digital Rights
Rue Montoyer 39/9, B-1000 Brussels
Tel:+32 (0)2 550 4112
E-Mail: brussels@edri.org, http://www.edri.org