ANEC-ICT-2014-G-020final
April 2014

ANEC comments on European Commission Standardisation request addressed to the European Standardisation Organisations in support of the implementation of privacy management in the design and development and in the production and service provision processes of security technologies

General Comments

ANEC welcomes the draft standardisation request on the implementation of privacy management in the design and development and in the production and service provision processes of security technologies, as we support the principle of "privacy by design and by default"[1].

Designing privacy and security in the development of technologies from the very beginning is essential to ensure that consumers' personal data protection rights are respected ("privacy by design"). Consumers expect the technologies they buy and use to protect their personal data by default, especially when it concerns their children[2]. To protect the rights of vulnerable consumers such as children, the highest level of personal data protection settings should be provided by default ("privacy by default"). Other users with less stringent requirements can then easily adapt the level of protection to their needs/wishes. As consumers often struggle with the complexity of modern technologies, systems where consumers are required to take actions to maintain their privacy will present greater risks than those where systems design privacy in a robust manner that does not require consumers' supplementary actions.

It is therefore essential that consumer participation in the standardisation work is ensured, and if the request is approved, ANEC expects to play a full part in the elaboration of the deliverable(s).

We think that Privacy by Design and by Default principles should be made very easy to implement, and that technologies and systems need very simple and clear requirements. A management system standard can document and manage the implementation of Privacy by Design, but by itself, it neither sets clear requirements nor helps system designers and engineers to understand the principle of and needs for Privacy by Design. Of course, in a management system standard in this field,

---

1 ANEC contribution to the European Commission public consultation on the Communication "A comprehensive approach on personal data protection in the European Union" (ANEC-ICT-2010-G-063final)

2 ANEC R&T study "The Standards Requirements for Consumer Internet Filtering Tools" (ANEC-R&T-2006-R-003).

there are going to be normative references to the European legislation on personal data protection. But such a translation of legal concepts into technical terms needs additional support, which should be provided by a standard (or part of a standard) that sets more detailed requirements.

This would also be in line with the European Parliament's 2010 opinion on standardisation mandates.[3] Therefore we suggest that requirements should clarify the policy goals the ESOs are expected to attain, so that they can focus on providing the technical means to reach policy goals. Defining requirements also reduces the risk of technical barriers to trade, which may stem from detailed technical regulations.

We welcome the possibility of commenting on this draft request at an early stage. Our comments focus on the parts that we consider as relevant from our field of activity, and we try to follow the same section numbering of the draft mandate/request, to aid the reader.

Specific Comments

Overall editorial consistency

We propose the Commission review carefully the editorial consistency of the document, for example there are some references requesting "the ESOs" carry out an action and others addressed to the "relevant ESO".

Title

This seems unduly long and complex, could we suggest: "...privacy management in relation to security services and technology"?

Foreword

We suggest to provide a clear definition of "security services and technology" as at the moment is not clear what is included or excluded. For example, would the e-banking system/software that consumers use at home or with their smart-phones fall under the scope of this request?

Second paragraph: delete sentence "following the abolition of prior notification to data protection authorities". Since the proposed Regulation will introduce a more focused checking according to Art. 34 and more deterring sanctions pursuant to Art. 79(6), this sentence may be misleading.

3

EU Parliament, 'Report on the future of European standardisation' 7.10.2010 A7-0276/2010 no 15, http://www.europarl.europa.eu/sides/getDoc.do?type=REPORT&mode=XML&reference=A7-2010-276&language=EN

3. Expire

We suggest changing the title of the heading to "Expiry/end of effect", as the word "expire" is a verb.

4.1.1 European standard for privacy management

Add the following aim:

-"Taking into account fundamental ethical and legal values, follow the legal principles of privacy and data protection and privacy goals such as pseudonymous identifiers, decentralised processing and anonymisation, in addition to specific technical and organisational requirements."

In ANEC's opinion, the draft request should include requirements that clearly separate policy and standards. The consideration of fundamental rights, data protection principles and privacy goals also ensures that the management system is comprehensive. This is necessary because privacy is only as good as its weakest link, and only the right "bundle of measures" can reduce the overall privacy impact and avoid that the impact of any component or interface of a security product or service is forgotten[4].

Add the following aim:

-"Creating flexibility for controllers to set design options appropriate for their individual case (full functionality)".

Art. 23(2) of the draft General Data Protection Regulation stipulates that the default configuration of a technical system must be privacy-friendly. This implies that PbD does not rule out the possibility of other configurations that do better achieve public security. The flexibility requirement also helps manufacturers to understand that PbD is not a limiting functionality but offers additional options for controllers to comply with the law and to create public acceptance, which is a market advantage compared to competitors and a unique selling proposition on the global market.

Add the following aim:

[4] Steinmüller 'Informationstechnologie und Gesellschaft' (Wiss. Buchgesellschaft Darmstadt 1993) 640.

-"Considering other crosscutting criteria such as IT security, usability, accessibility and cost effectiveness and therefore better integrating these into the manufacturer's overall product lifecycle".

To determine the level of achievement of privacy goals in a particular privacy management system the draft standards should show how manufacturers can integrate privacy into other policy goals such as accessibility and business goals such as reduction of implementation costs.

Add the following aim:

-"Assessing how the privacy management system will be demonstrated to controllers and supervisory authorities. The possibility of a PbD label shall be investigated. The standard shall deal with the verification of the management system by internal or external auditors."

As mentioned in the objectives of the draft request, the proposed standard aims to enable manufacturers to demonstrate PbD. This is also mentioned in the European Commission Communication of 26 July 2012 on Security Industrial Policy (termed an "EU security label")[5]. We also suggest that the Commission raises awareness of the privacy management system, and encourages authorities and policymakers to introduce the obligation in public procurement to prefer privacy certified products and services. This could be done in the requested Technical Report giving guidance on the implementation of privacy management.

Last paragraph:

It could be interesting to refer not only to "existing specifications and proven practices and approaches" but also to the results of relevant research projects and activities, as the stated aim of the request is to develop innovative solutions to comply with personal data protection legislation.

4.1.2 Technical Report giving guidance on the implementation of privacy management

Add following aim:

-"The ESO(s) shall assess the need for specific PbD standards on sectorial applications or technologies".

[5] (COM(2012) 417, p. 7).

As part of the guidelines for the practical implementation of the requested EN, we suggest that an assessment is made about the need for a more sectorial management systems/standards for specific technologies and applications such as biometrics. This could also be done in a CEN-CENELEC_ETSI Guide, which is not a standardisation deliverable as such, but instead provides guidance material to technical standards groups on how to handle "horizontal" topics consistently.

4.2.3 Development of the standards

We suggest that the ESOs should be requested to consult the National Data Protection Authorities represented in the Article 29 Working Party who should have the opportunity to provide advice on the elaboration of the standard either by direct involvement or requirement of endorsement. Moreover, the European Data Protection Supervisor is mainly responsible for implementation of Regulation 45/2001 on the processing of personal data by EU administration.

It is essential that dialogue between technical and data protection takes place. This is particularly important in a multidisciplinary context to ensure a feedback mechanism between technical and legal experts.

ANEC in Brief

ANEC is the European consumer voice in standardisation, representing and defending consumer interests in the development of technical standards, in the application of certification schemes to standards, and in the creation or revision of legislation on products and services. ANEC brings together national consumer organisations from the EU Member States, EFTA countries and Turkey and Former Yugoslavic Republic of Macedonia in order to define European positions on matters affecting consumer protection and welfare. ANEC receives funding from the European Commission and the EFTA Secretariat. In the EU context, consumers ensure that the public interest is represented in the standardisation work that complements European legislation and broader public policy initiative.