M/530

EUROPEAN
COMMISSION

Brussels, 20.1.2015
C(2015) 102 final

COMMISSION IMPLEMENTING DECISION

of 20.1.2015

on a standardisation request to the European standardisation organisations as regards European standards and European standardisation deliverables for privacy and personal data protection management pursuant to Article 10(1) of Regulation (EU) No 1025/2012 of the European Parliament and of the Council in support of Directive 95/46/EC of the European Parliament and of the Council and in support of Union's security industrial policy

COMMISSION IMPLEMENTING DECISION

of 20.1.2015

on a standardisation request to the European standardisation organisations as regards European standards and European standardisation deliverables for privacy and personal data protection management pursuant to Article 10(1) of Regulation (EU) No 1025/2012 of the European Parliament and of the Council in support of Directive 95/46/EC of the European Parliament and of the Council and in support of Union's security industrial policy

THE EUROPEAN COMMISSION,

Having regard to the Treaty on the Functioning of the European Union,

Having regard to Regulation (EU) No 1025/2012 of the European Parliament and of the Council of 25 October 2012 on European standardisation, amending Council Directives 89/686/EEC and 93/15/EEC and Directives 94/9/EC, 94/25/EC, 95/16/EC, 97/23/EC, 98/34/EC, 2004/22/EC, 2007/23/EC, 2009/23/EC and 2009/105/EC of the European Parliament and of the Council and repealing Council Decision 87/95/EEC and Decision No 1673/2006/EC of the European Parliament and of the Council[1], and in particular Article 10(1) thereof,

Whereas:

(1) The Charter of Fundamental Rights of the European Union recognises in Article 8 the right to the protection of personal data. To this end Article 8 (2) of the Charter sets out the principles of fair and purpose bound data processing, the necessity of consent or a legitimate basis laid down by law for such processing and the right to access to such data as well as their rectification by the person concerned. This fundamental right is developed by the European legal framework on the protection of personal data consisting in particular of the Data Protection Directive 95/46/EC[2], the ePrivacy Directive[3] and the Data Protection Regulation (EC) No 45/20013 relating to processing by Union institutions and bodies[4].

(2) The currently applicable Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data[5] sets up general principles on the protection of personal data.

---

1 OJ L 316, 14.11.2012, p. 12.

2 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23.11.1995, p. 31.

3 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L 201, 31.07.2002, p. 37.

4 Regulation (EC) 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, OJ L 8, 12.1.2001, p. 1-22.

5 OJ L 281, 23.11.1995, p. 31.

(3) The Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)[6], equally foresees that processing of personal data will have to be realised following a "data protection by default and by design" approach. The Regulation emphasizes inter alia that standards should help the development of products including the Privacy by default and by design principle, following the abolition of prior notification to data protection authorities.

(4) Under the action 8 of the Communication of 26 July 2012 entitled: "Security Industrial Policy"[7], the Commission committed to issue a mandate to the European standardisation organisations to develop a standard, modelled on existing quality management schemes, but applied to the privacy management in the design and development and in the production and service provision processes of security technologies.

(5) A standardisation request in support of the implementation of privacy management is included in point 2.2.14 of the annual Union work programme for European standardisation[8].

(6) The European standardisation organisations, the European stakeholder organisations receiving Union financing have been consulted.

(7) The measures provided for in this Decision are in accordance with the opinion of the Committee established by Article 22 of Regulation (EU) No 1025/2012.

HAS ADOPTED THIS DECISION:

Article 1

The European Committee for Standardisation, the European Committee for Electrotechnical Standardisation and the European Telecommunication Standards Institute are requested to draft European standards and European standardisation deliverables as set out in the Annex to this Decision.

6 COM(2012) 11 final
7 COM(2012) 417 final
8 COM(2013) 561 final

Article 2

This Decision is addressed to the European Committee for Standardisation (CEN), the European Committee for Electrotechnical Standardisation (Cenelec) and European Telecommunications Standards Institute (ETSI).

Done at Brussels, 20.1.2015

For the Commission
Dimitris AVRAMOPOULOS
Member of the Commission

CERTIFIED COPY
For the Secretary-General,

Jordi AYET PUIGARNAU
Director of the Registry
EUROPEAN COMMISSION

EUROPEAN
COMMISSION

Brussels, 20.1.2015
C(2015) 102 final

ANNEX 1

ANNEX

to Commission implementing decision

Standardisation request addressed to the European standardisation organisations in support of the implementation of privacy and personal data protection management in the design and development and in the production and service provision processes of security technologies

Table of Contents

Foreword

The demand for and use of security technologies has increased over years, resulting from experienced or perceived threats to security, and supported by the overall technical progress. In that respect, anti-terror legislation has been the main driver for the development and deployment of security technologies. With the growth of this activity sector, but also generally the volume of personal data being collected, processed, stored, and shared has dramatically increased. At the same time, public opinion expresses more and more the need to protect such data, to drastically improve the transparency of how this data is being handled, and to reduce intrusions into the privacy of an individual to a minimum. The security industry has thus to face a growing challenge: improving the protection of privacy and personal data, while meeting the requirements of their customers.

Whilst legally speaking the customers of the security industry often bear the legal responsibility for complying with data protection rules (being the data controllers), their providers also bear some responsibility for data protection from a societal and ethical point of view. These involve those who design technical specifications and those who actually build or implement applications or operating systems.

The Charter of Fundamental Rights of the European Union[1] enshrines in Article 7 privacy and recognises in Article 8 the right to the protection of personal data. This fundamental right is developed by the European legal framework on the protection of personal data consisting in particular of the Data Protection Directive 95/46/EC[2] , the ePrivacy Directive[3] and the Data Protection Regulation (EC) No 45/20013 relating to processing by Union institutions and bodies[4] . They lay down several substantive provisions imposing obligations on the data controller and recognizing rights to the data subject, prescribing sanctions and appropriate remedies in cases of breach, and establishing enforcement mechanisms to make them effective. This objective of this legal framework is to minimise the processing of personal data, and using anonymous or pseudonymous data where possible.

In its Communication on Promoting Data Protection by Privacy Enhancing Technologies (PETs)[5] , the Commission considers that PETs should be developed and more widely used, in particular where personal data is processed through ICT networks. The Commission considers that wider use of PETs would improve the protection of privacy as well as help fulfil data protection rules.

Directive 95/46/EC sets out a range of obligations to protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the

1 OJ C 326, 26/10/2012, p. 391

2 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23.11.1995, p. 31.

3 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L 201, 31.07.2002, p. 37.

4 Regulation (EC) 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, OJ L 8, 12.1.2001, p. 1-22.

5 COM (2007) 228.

processing of personal data. The person or body which determines the purposes and means of the processing of personal data ('controller') must ensure, amongst other, that personal data is processed lawfully, collected for specified, explicit and legitimate purposes and kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or further processed. Recently, the Commission proposed a Regulation on the protection of individuals with regard to the processing of personal data and on the free movement of such data[6] which requires explicitly that processing of personal data will have to be realised following a 'data protection by default and by design' approach.

Stimulating privacy by design initiatives is also supported in the cybercrime strategy released in 2013[7], which invites public and private stakeholders to stimulate the development and adoption of industry-led security standards, technical norms and security-by-design and data protection-by-design principles by ICT product manufacturers and service providers. As the existing and future legal instruments on data protection are technologically neutral, standards are useful and needed for specifying how the legal instruments will be implemented.

This standardisation request builds on the longstanding consensus[8] that it is important to embed data protection requirements into the technical design specifications, business practices, and physical infrastructures aiming at safeguarding the data protection rights of individuals. It should be noted that data protection and privacy issues does not only relate to the technical domain, but also to other domains of societal interaction, e.g. the protection of the personal integrity of an individual, the protection of related, personal information, of personal living circumstances.

The Commission considers that, given the complexity of security technologies, standards, structured according to international standards on quality management systems, and covering the way manufacturers and service providers should address privacy and personal data protection management issues in their design and development and production and service provision processes of products and services, should be put in place. Such standards would provide an indication for the preparation, implementation, monitoring and revision of a dedicated management process for privacy issues to be taken into account in each step of the design and development and production and service provision processes of security technologies and services, which would contribute to privacy management and improve both the efficiency and the social acceptance of EU security related products. Furthermore, such standards may be important to boost consumer confidence in security technologies.

6 COM (2012) 11 final

7 Joint Communication on the cybercrime strategy, p.13: JOIN(2013) 1 final

8 The importance of supporting the development of tools for data protection by design and by default was already developed the COM Communication on Privacy enhancing technologies: COM(2007) 228 final

1. OBJECTIVES

1.1. Requested standardisation activities

The Commission requests the European standardisation organisations (ESOs) in accordance paragraphs 1 and 2 of Article 10 of Regulation (EU) No 1025/2012 to draw up:

(1) One or more European standards, which shall cover the following aspects:

− How to address and manage privacy and personal data protection issues during the design and development and the production and service provision processes of security technologies and services, allowing manufacturers and service providers to develop, implement and execute a widely recognised "Privacy by Design" (PbD) approach in their processes.

and

(2) One or more related European standardisation deliverable(s)

− Addressed to the manufacturers and service providers when specifying the privacy and personal data protection management processes with an explanation how to realise them, including descriptions of the necessary roles, tasks, documentation, hardware and software requirements, and templates to be used when applying the requested standard(s).

1.2. Public interests and policy objectives

Article 8 of the **Charter of Fundamental Rights of the EU**[9] enshrines protection of personal data as a fundamental right. There is a widely recognised need for better integration of the 'societal dimension' into security-related activities in order to reduce the uncertainty of the societal acceptance of such activities. Security technologies and services aimed at enhancing privacy should allow the security industry to develop widely acceptable security products and services, and thus a competitive edge over other security products and services. Enhanced privacy management would not only ease the compliance with and respect for fundamental rights but would allow for an efficient use of R&D investments as well as allowing the demand side to purchase products and services which fulfil entirely their security and data protection specifications thus being better accepted by the society.

Article 16(1) of **Treaty on the Functioning of the European Union (TFEU)**[10], as introduced by the Lisbon Treaty, establishes the principle that everyone has the right to the protection of personal data concerning him or her. Moreover Article 16(2) of the TFEU introduces a specific legal basis for the adoption of rules on the protection of personal data. **The [proposed] Regulation on the protection of individuals with regard to the processing of personal data and on the free movement of such data (*General Data Protection Regulation*)**[11], and repealing Directive 95/46/EC, relies on this new legal basis in the Treaty.

The current Directive 95/46/EC stipulates that personal data must be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. The proposal for the General Data Protection Regulation builds on this further by establishing the principle of "data protection by design and by default". In light of this, it is

9 OJ C 326, 26/10/2012, p. 391

10 OJ C 326, 26/10/2012, p. 47

11 COM (2012) 11 final: Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation).

essential that products, systems and services are initially designed and developed as well as produced and provided according to principles of "data protection by design and by default". The aim of this standardisation request is to provide voluntary tools to manufacturers and service providers to allow them to demonstrate to controllers using or utilizing their products and services, that their products or services have been designed and developed as well as produced and provided duly respecting "data protection by design and by default" -principles in order to ensure personal data protection.

In its **Communication[12] of 26 July 2012 on "Security Industrial Policy"** the Commission presented actions to strengthen the innovativeness and competitiveness of the European security industry. Specific attention was paid to ethical concerns, notably privacy issues, in the context of security products. In order to address these issues, the Commission aims to encourage the integration of "Privacy by Design" and "Privacy by Default" concepts at the early stages of the design and development and production processes of security technologies by means of voluntary European standards. Therefore this standardisation request implements Action 8 of the Communication to ensure availability of such European standards.

2. ACCEPTANCE OF THE REQUEST

The ESOs are asked to inform the Commission within one month after the receipt of this request whether they accept it. Conditional acceptance is considered as refusal.

The acceptance reply may include a request for Union funding or may indicate if Union funding available for activities pursuant to Article 15 of Regulation (EU) No 1025/2012 is applied for later and informing also on estimated amount needed and estimated date for a possible request. Such a funding request shall respect deadlines set in this standardisation request and in the mandated work programme, as agreed with the Commission according to point 5.4, for the execution of the standardisation work.

3. EXPIRATION

Where the standardisation request is not accepted by any of the ESOs, this request shall expire three (3) months after the notification of this Decision to the ESOs.

This request, if accepted by relevant ESOs, shall expire after relevant ESOs submit, according to point 5.5, the final report indicating the completion of this request.

4. DESCRIPTION OF THE REQUIREMENTS FOR THE REQUESTED DELIVERABLES AND FOR THE STANDARDISATION WORK

4.1. Requirements for the deliverables

4.1.1. European standard(s) for privacy and personal data protection management

The requested European standard(s) for the design and development and for the production and service provision of security products and services shall be modelled to be compatible with EN ISO 9001[13] on quality management systems in order to allow integrate privacy and personal data protection management as an integral part of quality management.

The standard(s) shall aim at:

[12] COM (2012) 417,

[13] EN ISO 9001:2008, Quality management systems. Requirements

– Providing a clear definition for security products and services as referred in section 2 of the Commission Communication on Security Industrial Policy

– Translating the concept of "Privacy and personal data protection by Design" into concrete indications for manufacturers and service providers to plan, implement, control and revise a management process appropriately addressing privacy needs and requirements in each step of the design and development and production and service provision of security technologies and services.

– Taking into account the existing European privacy risk management methodologies used to build privacy and personal data protection impact assessments[14].

– Taking into account the international standards on information security management (like ISO/IEC 27001[15] and ISO/IEC 27002[16])

– Taking into account the international standards on risk management that already exists or are under development.

– Providing the security industry with guidelines and instructions for the design and development and for the production and service provision of security technologies and products, in order to facilitate compliance with the provisions of Directive 95/46/EC and if adopted, the General Data Protection Regulation, without prejudice to any further criteria and requirements that might be put in place pursuant to its entry into force.

– Allowing manufacturers, service providers and to build up their privacy management policies which compliance can be assessed against the specifications given in the requested European standard(s).

– Allowing the European security industry to have access to a dedicated European standard on privacy and personal data protection management and thus promoting their positions as pioneers in implementing the privacy and personal data protection management approach and by this to gain a competitive advantage within and outside the EU with regard to this sensitive subject of highest public concern. At the same time by making sure that standardisation in this context will not hinder technological advancements and innovation,

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

– Taking into account processes for collaborative/participatory design of ethical and legal values in order to increase transparency and to improve citizens' trust such as 'privacy in design'[17]

---

[14] Such as the privacy impact assessment for RFID applications http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp180_annex_en.pdf and the EG2 report on data protection recommendations for smart grids: http://ec.europa.eu/energy/gas_electricity/smartgrids/doc/expert_group2.pdf, as well as the result PIA framework, to be published by the EU expert group on smart grids.

[15] ISO/IEC 27001, Information technology— Security techniques — Information security management systems — Requirements

[16] ISO/IEC 27002, Information technology – Security techniques – Code of practice for information security management

[17] EUROPEAN GROUP ON ETHICS IN SCIENCE AND NEW TECHNOLOGIES, Ethics of Security and Surveillance Technologies, Opinion 28, Brussels, 20 May 2014: "Privacy in Design is distinct from PbD in that it concerns itself primarily with raising awareness about the processes through which values

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

– 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.

– The standard(s) shall deal with the verification of the management system by internal and external auditors.

The requested European standard(s) shall be preferably based on existing specifications and proven practises and approaches[18] already tested and implemented in the market. Relevant existing standardisation work programmes initiated in ISO/IEC context as well as other existing examples at national and European level should be examined. A specific attention should be paid to build the requested European standard(s) in way that it supports international standardisation activities of ISO/IEC JTC 1[19] in the field of data protection and other European standards dealing with data protection[20].

The general framework for setting privacy implementing measures for products to be followed in the requested European standard(s) is given in Appendix IV.

4.1.2. European standardisation deliverables(s) giving guidance on the implementation of privacy and personal data protection management

The requested European standardisation deliverables(s)[21] shall give guidelines for the practical implementation of the requested European standard(s).

The deliverables(s) shall aim to detail:

– Provision of a clear definition of security services and technologies.

– Information on the overall privacy and personal data protection management process and its implementing measures.

– Guidance how to establish associated building blocks for the formulation of a dedicated privacy and personal data protection management policy at the level of the manufacturer and service provider.

– Guidance on the individual roles, tasks and training needs of company staff involved in privacy and personal data protection management process.

– Guidance on the individual documentation steps of the measures implemented, on how to build the reporting templates and any other templates needed.

– Guidance on verification, storage and auditing requirements related to the documentation and reports produced during the design and development and the

---

and norms become embedded in technological architecture. Privacy in design looks at the normativity of structural choices in an effort to promote transparency and protect rights and values of the citizens." (p.32 and Recommendation 15 at p.91)

18 Further information on privacy and data protection frameworks for specific technology and on studies and reports is given in Appendix III.

19 ISO/TC JTC 1/SC 27 “IT Security techniques” http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_tc_browse.htm?commid=45306

20 Like European standardisation activities related to the Commission standardisation request M/463 of 8 December 2008 on “Radio Frequency Identification (RFID) and Systems”, http://ec.europa.eu/enterprise/standards_policy/mandates/database/index.cfm?fuseaction=search.detail&id=415#

21 However these deliverables can also be published as European standards.

manufacturing and service provision processes of security related products or services.

4.2. Requirements for the standardisation work

4.2.1. Project planning

The relevant ESO shall ensure that an appropriate and continuous overall project planning is in place for the execution of this standardisation request. A joint work plan which describes, among others things, tasks, milestones, estimated or allocated resources, estimated or actual deadlines and timeframes as well as contact points shall be made available to the Commission.

4.2.2. Provision of the work programme

On the basis of the requirements given in this request and according to Appendix I to this request, the relevant ESO(s) shall prepare **a joint preliminary work programme** indicating all requested work items, responsible technical bodies and a tentative timetable for the execution of the work.

It is under the discretion of the relevant ESO(s) to decide how many work items for standardisation are established and how many European standards and European standardisation deliverables are needed in order to implement the requested work programme as given in the Appendix I.

4.2.3. Development of standards

The **joint mandated work programme** as agreed according to point 5.4 will be the basis for the standardisation work.

During the standardisation work the ESOs shall consult the references to privacy by design by the European Data Protection Supervisor (EDPS)[22] and consult with the Article 29 Working Party

The relevant ESO(s) shall report annually to the Commission on the execution of the mandated work programme.

5. ARRANGEMENTS FOR THE EXECUTION OF THIS REQUEST

5.1. General conditions for executing this standardisation request

General conditions for the execution of the Commission's standardisation requests apply during the standardisation work.

5.2. Project planning

The **joint work plan** shall be made available to the Commission at the same time when providing the preliminary work programme and communicating annual reports according to points 5.3 and 5.5.

5.3. Provision of the work programme

The **joint preliminary work programme** shall be sent to the Commission no later than **ten (10)** months after the notification of this Decision by the Commission.

[22] Information on EDPS's references to privacy by design see: Appendix II.

5.4. Agreement on the mandated work programme

The Commission will inform relevant ESO(s) no later than **one (1)** month after receiving the joint preliminary work programme on the work items to be included in the mandated work programme including any priorities to be observed during the work.

5.5. Reporting

The relevant ESO(s) shall give **the first joint annual report fourteen (14)** months after the notification of this Decision by the Commission and then after **every twelve (12)** months.

The relevant ESO(s) shall give the joint **final report** three (3) months after publishing all the deliverables requested by this mandate in order to notify the completion of this standardisation request.

5.6. Other provisions

The relevant ESO(s) shall maintain continuous liaisons with the Commission services responsible for this standardisation request during the execution of the request.

Possible disagreements and disputes on the interpretations of the requirements given in this standardisation request shall be addressed to the Commission services responsible for this standardisation requests and always informing the standardisation unit of Enterprise and Industry Directorate General.

APPENDIX I
Requested Work Programme

Reference information (title, subject matter, source document, technical body etc.)	**Deadline for publication**[23]
1. **European standard(s)** addressing privacy management in the design and development and in the production and service provision processes of security technologies (see point 4.1.1)	48 months after the notification of this Decision to the ESOs
2. **European standardisation deliverable(s)** giving practical guidelines for the practical implementation of the requested European standards(s) (see point 4.1.2)	48 months after the notification of this Decision to the ESOs

[23] "Publication" makes reference to the moment when the relevant ESO makes a standard (or another deliverable) available for its members or to the public.

APPENDIX II
References to Privacy by Design by the European Data Protection Supervisor

The European Data Protection Supervisor (EDPS)[24] defines Privacy by Design (PbD) as "integration of data protection and privacy from the very inception of new products, services and procedures that entail the processing of personal data". Through its various opinions[25] it has given some guidelines on the way this concept should be applied:

- According to the EDPS Privacy by Design is particularly an element of accountability.
- The EDPS has made clear that PbD should be technologically neutral, and that it should not intend to regulate technology, i.e. it should not prescribe specific technical solutions. On the contrary existing privacy and data protection principles should be integrated into ICT systems and solutions. PbD requirements should apply across sectors, products and services.
- PbD includes technical and organizational measures, both at the time of the design of the processing system and at the time of the processing itself, particularly in order to ensure the protection of personal data and prevent any unauthorized processing.
- In its opinion on the Turbine Research Project[26] the EDPS considers that the partners of the project have committed to comply with the PbD principle as they provided a detailed document with legal requirements, intertwined with functional and technical requirements, which was prepared during the first months of the project. The EDPS has welcomed the project as it demonstrates that implementing PbD as a key principle in research is an effective measure to ensure "privacy compliant" solutions. PbD extends not only to the design and technical solutions of ICT systems, but it comprises the various steps in the set-up of the project and its organizational practices. This latter aspect can be achieved by ensuring legal compliance, implementing the required data protection principles, and by implementing procedures and training developed to ensure correct information and training of all the parties involved. Moreover, the demonstrators provide the possibility to test the advantages of the implementation of the principle in real case scenarios.

---

24 Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions - "A comprehensive approach on personal data protection in the European Union".

25 Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions - "A comprehensive approach on personal data protection in the European Union"; Opinion of the European Data Protection Supervisor on Promoting Trust in the Information Society by Fostering Data Protection and Privacy.

26 Opinion of the European Data Protection Supervisor on a research project funded by the European Union under the Seventh Framework Programme (FP7) for Research and Technology Development - Turbine (TrUsted Revocable Biometric IdeNtitiEs).

APPENDIX III
Information on existing privacy and data protection frameworks for specific technology including studies and reports referring to "Privacy by Design"

Existing privacy and data protection frameworks for specific technologies

When developing the future PbD standards, existing frameworks for specific technologies should be taken into account, such as the one for security scanners. To that respect, the Commission in its Communication of 15 June 2010 on the use of Security Scanners at EU airports[27] stressed that PbD and Privacy Enhancing Technologies (PETs) applied to hardware and software incorporated in security scanners may produce information and communication systems and services minimizing the collection and the processing of personal data. Such systems would ensure, for example, that images are not stored (retained), copied, printed, retrieved or sent remotely, that unauthorized access is prevented, and that images that are analyzed by a human reviewer are not linked to the identity of the screened person and are kept 100% anonymous.

Studies and reports referring to Privacy by Design

Meanwhile a number of studies and reports in Europe refer directly to the PbD principle and the need to implement it in the security sector. Exemplary, a 2008 report of the UK Information Commission Office (ICO) developing recommendations with the view to help organizations to implement the Privacy by Design principle[28], based on managerial, organizational and technical measures, as well as the report of ESRIF (European Security Research and Innovation Forum)[29] and the study delivered to the Commission by ECORYS on the Competitiveness of the EU security industry[30] are mentioned here, the latter both from 2009.

27 COM (2010) 311 final

28 http://www.ico.org.uk/for_organisations/data_protection/topic_guides/~/media/documents/pdb_report_html/PRIVACY_BY_DESIGN_REPORT_V2.ashx

29 http://ec.europa.eu/enterprise/policies/security/files/esrif_final_report_en.pdf

30 http://ec.europa.eu/enterprise/policies/security/files/study_on_the_competitiveness_of_the_eu_security_industry_en.pdf

APPENDIX IV
Product lifecycle and privacy implementing measures under the responsibility of a manufacture

The requested European standard(s) shall identify typical privacy issues and questions to be taken into account during the phases of **product definition**, **design**, **development**, **system integrations** and, as appropriate, of **testing** as outlined in Figure 1. (e.g. as "privacy implementing measures").

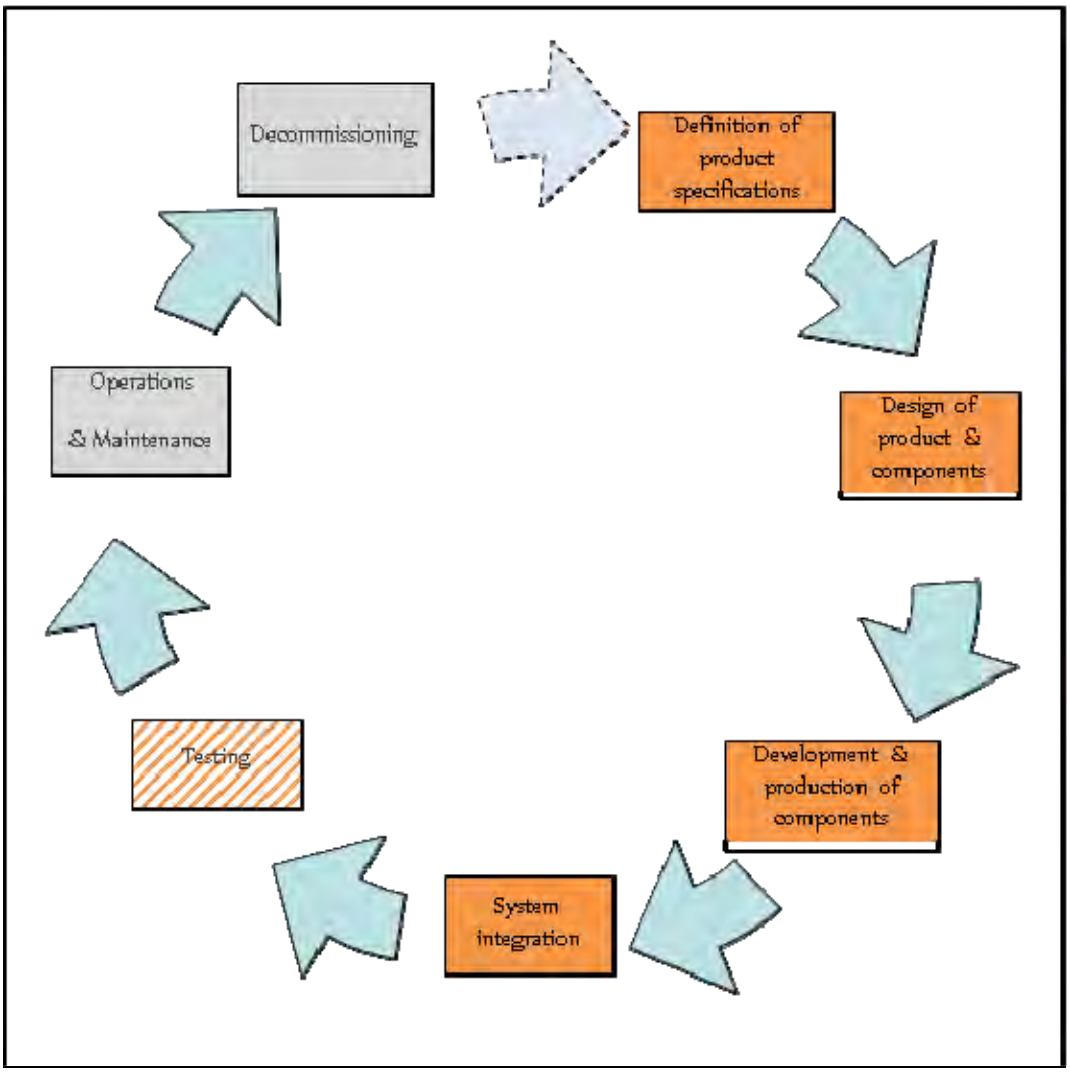

Figure 1: A generic product lifecycle and phases to be covered by the requested European standard(s)

Typical privacy issues to be tackled in each phase include:

– **Definition of product specifications**: identification and definition of privacy requirements and constraints, according to the specific product expected exploitations and the type of data documentation of the privacy specifications;

– **Design of product and components**: allocation of the privacy requirements and constraints to individual components; documentation of the allocation;

– **Development and production of components**: verification and documentation that the allocated privacy requirements and constraints have been implemented accordingly;

– **System integration**: verification and documentation that through the integration of the individual components into the final product/system, and more over through the potential integration of further, external components (e.g. commercials off the shelf (COTS)) including ICT and software the originally specified privacy requirements and constraints are still fully implemented and respected.

– **Testing**: an important phase of product/service development lifecycle may often involve processing personal data and interconnected risks.

The proposed scheme, for each step of the product lifecycle, should identify the relevant data protection risks and propose solutions for their mitigation or, possibly, measures to void the identified risks.