Business Plan for CEN/ISSS Workshop Data Protection and Privacy (CEN/ISSS WS/DPP)

1 Document status

Version 2.0: As adopted at the Kick-Off meeting on 3 July 2003

2 Proposers (companies, organization, etc.)

ACS
AFNOR
ANEC
BSI
ChevronTexaco
Custodix NV
DaimlerChrysler AG
Deutsche Telekom AG
€NIX@agency
EuroCommerce
Fujitsu Limited
IFPI
IMS Health
LawIDs
Lios Geal Consultants
PricewaterhouseCoopers
The Information Commissioner, UK
Shell
SQS

3) Workshop objectives

The Workshop will implement various recommendations of the Report of the IPSE Steering Group under mandate M/289 (background and recommendations at Annex A).

This Report made a number of specific recommendations for consensus-building within a CEN/ISSS Workshop, as well as other recommendations where the forum for activities was not specified.

In addition, the Workshop will take due account of the business and security requirements of the data protection-related aspects of CEN/ISSS WS/eTrust specifying regulatory and self-regulatory requirements for commercial transactions on line. It will specifically deal with the chapter on data protection.

The Workshop will aim to use the standardization process to help organizations to comply with the Data Protection Directive and relevant national legislation by facilitating harmonization of practice, developing the understanding and predictability of detailed or sector practices, contributing to resolving ICT technical compliance issues, and encouraging consistency of assessment and oversight.

The Workshop will have due regard to the provisions of the relevant EU legislation on data protection and privacy, including Directives 95/46/EC, and 2002/58/EC.
The Workshop will seek to prepare a number of deliverables itself, but in addition it will act as an open discussion forum concerning those recommendations that are not specifically addressed to CEN/ISSS. It may make proposals and address these to the appropriate organizations.

4) Detailed Workshop contents, deliverables and timescales

Work Area A: Best practice and guidance

A1. Generic set of contract clauses

In relation to Recommendation 3 of the IPSE Report, the Workshop will prepare a **generic set of contract clauses** reflecting the requirements of Article 17 of Directive 95/46 for use within the EEA. The results will be published in the form of a CEN Workshop Agreement. The Workshop will be assisted in this activity by a Project Team of experts appointed under CEN/ISSS Workshop rules, which will prepare draft material for its consideration.

The Workshop will be assisted by a Project Team of experts appointed under CEN/ISSS Workshop rules, which will prepare draft material for its consideration.

Start of work December 2003
Stable draft June 2004
CWA September 2004

A2. Common European voluntary best practices for data controllers

It will identify the requirements for a set of **common European voluntary best practices** for data controllers, in relation to Recommendation 1 of the IPSE Report. At that point, the Workshop may decide to progress these into a further CWA.

The results will be published as a CEN Workshop Agreement.

Start of work December 2003
Stable draft June 2004
CWA September 2004

In order to achieve these tasks, the Workshop will make and maintain an inventory of the voluntary codes of conduct, privacy statements and best practices at National, European and International level as well as an inventory of the legal requirements for data controllers at national, European and International level. This task will cover the off line and online world. For the latter the work performed by CEN/ISSS WS/eTrust could be useful.
Work area B: Assessment of data protection audit practice

In response to Recommendation 4 of the IPSE Report, the Workshop will prepare an inventory of data protection auditing practice to record best practice in this area, and assess the extent to which the practice of data protection audit could benefit from standardization.

Start of work September 2003
Agreement to proposals for further activity January 2004

The Workshop will be assisted by a Project Team of experts appointed under CEN/ISSS Workshop rules, which will prepare draft material. Any further activities to be carried out in CEN/ISSS will be subject to the agreement of the Workshop and amendments to the present Business Plan at that stage.

Work Area C: Web seals and technologies

C1 Survey of web seals programmes

In response to Recommendation 5 of the IPSE SG Report, the Workshop will prepare an informational survey of currently operational web seals programmes, and make appropriate recommendations concerning standardization aspects. The Workshop would analyse the possibilities for consensus on good practice concerning web seals programmes. The results will be published as a CEN Workshop Agreement.

Start of work September 2003
Detailed scope available for consideration by Workshop Plenary November 2003
Stable draft available for consideration by Workshop Plenary March 2004
Approval of CWA by Workshop Plenary June 2004

C2 Technology impact analysis

In response to Recommendation 6 of the IPSE SG Report, the Workshop will prepare an impact analysis of data protection technologies, with recommendations for longer-term co-ordinated advice to regulators, and recommendations to ensure that standards take account of the state of the art in this area. The results will be published as a CEN Workshop Agreement.

Start of work September 2003
Detailed scope available for consideration by Workshop Plenary November 2003
Work Area D: Measures to improve Awareness

In response to Recommendation 7 of the IPSE SG Report, the Workshop will prepare a report on measures to improve awareness of the data protection Directives and the means to implement them, aimed especially at SMEs and consumer organizations. The Workshop will be attentive to the complexity of the data protection field. In the transposition of the 1995 Directive at national level, different national interpretations of the detailed requirements have inevitably resulted in discrepancies, and businesses trading across frontiers require appropriate guidance on what these differences imply. The Workshop should take into account the report of DG Internal Market on the implementation of the Directive.

Start of work September 2003
Detailed scope available for consideration by Workshop Plenary November 2003
Approval of report by Workshop Plenary March 2004

5 Resource requirements

Workshop Chairman

This is a voluntary function, estimated at 20 man-days; the Chair will be appointed by the Workshop Kick-Off meeting.

Workshop Secretariat

This function will be carried out by a CEN Member organization, to be appointed at the Workshop Kick-Off meeting. It is estimated that 42 man-days will be required funded by the registered participants of the Workshop, which will pay a fee of 600 EUR and by the EU and EFTA under the eEurope Standards Action Plan.

Workshop Working Groups

These will depend on the voluntary effort of registered Workshop participants, together with a total of 154 man-days of paid Project Team resource, funded by the European Commission and EFTA Secretariat under the eEurope Standards Action Plan. The amount of man-days to be assigned to each Project Team will be specified in detailed Terms of Reference to be approved after the Workshop Kick-Off meeting.

6 External liaisons
A liaison will be established with ETSI Project M-Commerce (EP/MC).

7 Contact points

Nick Mansfield
Shell Information Technology International B.V.
nick.mansfield@shell.com

James Boyd
Strategy Manager, CEN/ISSS
james.boyd@cenorm.be
Annex A  Background and recommendations of the IPSE report

A1  Background

The objective of The Initiative for Privacy Standardization in Europe (IPSE) was to analyse the current status of privacy protection efforts and determine whether standardization actions in the broadest sense could benefit the processes and implementation of the European Data Protection Directive 95/46/EC. The report, prepared by an IPSE Project Team and approved by the IPSE Steering Group, looked at the background and a broad representative sample of the current work in progress on data protection. It is available on the CEN/ISSS website at http://www.cenorm.be/isss/Projects/DataProtection/IPSE/ipse_finalreport.pdf. It was intended to stimulate comments about the way forward from a wide constituency so that the final report and recommendations provide the required information for reasoned decision making by the European Standards organizations. The report concluded that there was sufficient basis for specific standardization initiatives. Seven recommendations were proposed as follows.

Management Practices
- Identify a common European set of voluntary best practices for data protection
- Do not initiate management standards, monitor developments in ISO/COPOLCO
- Develop a generic set of contract clauses and terms for article 17

Assessment and Verification
- Prepare an inventory of data protection auditing practices
- Conduct a survey of web seals as a basis for considering further standardization work in this area

Impact on Privacy of Technologies
- Report and process on impact of technologies on Data Protection, including Privacy Enhancing Technologies (PETS)

Consumer Education
- Privacy standards education and promotion

The document was designed to be of manageable scope and length while providing a realistic context for public debate and subsequent action. It was not intended to be an exhaustive and fully documented analysis of the possible scope for standardization. CEN/ISSS held a first Open Meeting on this subject on 23/24 March 2000, for which it commissioned a study by Professor Jos Dumortier and Caroline Goemans of the University of Leuven. Readers of this report are urged to read the Dumortier report¹, as an important element of background material. A preliminary draft of the present report was issued for public review in July 2001, and comments were requested. The Project Team attempted to incorporate all contributions into the body of a revised discussion draft, which was issued on September 19, 2001. An Open Meeting was held in Paris on September 27, and further comments were invited. The summary of the discussion at this Meeting is attached to this report, and has been taken into consideration in the final report.

A2  Recommendations

Recommendation 1 – Voluntary Best Practices

Identify a common European set of voluntary Best Practices for data protection and make this available freely or at low cost to help businesses and data managers ensure that they are compliant with the Directive and, where possible and appropriate, the diverse European national laws and additional requirements. This guide would be applicable generally across all sectors, but may need to be supplemented by sector specific advice at a later stage, such as for human resources information, or for online advertising.

Recommendation 2 – Management Standard

Do not initiate management standards, especially in the sense of those involving a formal certification which large parts of the market do not appear ready to accept. Any steering group established to implement recommendations resulting from this study should also monitor continuing developments in this area in ISO/COPOLCO.

**Recommendation 3 – Generic Contract Clauses and Terms**

Develop a generic set of contract clauses reflecting the requirements of Article 17 of Directive 95/46/EC for use within the EEA.

**Recommendation 4 – Inventory of Data Protection Auditing Practice**

Prepare an inventory of data protection auditing practice to record best practice in this area, and to assess the extent to which the practice of data protection audit could benefit from standardization. The study should consider current auditing practices and draw input from all stakeholders, including Data Protection Commissioners, those currently offering data protection audit services, representatives of auditing organisations, security and legal experts, and organisations which have used audit.

**Recommendation 5 – Conduct a survey of web seals as a basis for considering further standardization work in this area**

The survey would ascertain the role played by seals, how the different web seal programmes work and how seals contribute to the development of consumer trust. The survey will be used as a basis for deciding whether common standards could be developed for seals, possibly to guarantee the delivery of minimum standards in seal programmes.

**Recommendation 6 – Analysis of the impact of technologies on data protection, coordination and the initiation of longer term processes**

Develop a coherent approach to the assessment of the impact of ongoing technological development on the implementation of the Directives, with a view to ensuring a better dialogue between the standards developers and the technical community, and the oversight authorities and consumers. This approach is seen as having three components:

1. The initial requirement here is to develop a technical report, based on stakeholder requirements and an analytical framework26, which can be used to understand and give context to the impact of technologies and standards, and the potential for improvement of outcomes through the use of PETS.

The framework will be a valuable tool to educate and assist stakeholders in their practical understanding of the potential and expected impact of new and emerging technologies and PETs, including systems and related standards, and provide a snapshot to assist data protection commissioners and others to keep up to date on technological developments.

2. We propose also that the report make recommendations concerning the establishment of a longer-term coordination system for the main involved players of new developments in technology, and ensure that there is an “early warning system” in place. This would assist data protection commissioners and others to keep up to date on technology developments, it would assist them in their oversight roles, and would ensure independent data protection expertise and analysis for the technology.
3. An additional aspect concerns the standardization process itself. The report would help advise standards groups of the "state of the art", but it is also for consideration whether an agreed process should be put into place, at least within the European Standardization Organizations, to ensure that future standardization is better able to take account of these issues, given the legal requirements. We therefore recommend that the report outline such a process, that could provide the capability for an ongoing analysis of new developments in the technologies, and for an "early warning system" to ensure standards groups in such key areas as cookies, wireless, geolocation tracking and location-based services, can take account of these developments and better reflect the legal and policy concerns identified by data protection authorities.

Recommendation 7 – Privacy standards education and promotion

Compile and deliver through multiple-channels, including the internet, a targeted range of educational and guidance material on privacy-related standardization issues. This would establish a focal point for consumer education, assessing, and promulgating the usefulness of standards activity in addressing the trust and privacy concerns of individuals in their various roles as citizens, consumers etc. Whether staffed by an individual or through some collective endeavour, the job would be to promote and ensure that information materials are accessible and relevant to consumer needs, that can be used by local and national training programmes organized by schools, third level institutions, adult education institutes, national standards organizations, privacy advocacy associations, data protection offices, consumer associations etc.

Note: This recommendation would use as raw material the deliverables from standardization initiatives, including those resulting from the other recommendations in this report. It is important however to have representation from the targeted stakeholders including citizens, consumers, educators, industry, service providers, public administrations, data protection authorities and legislators participating in the promotion activities recommended here.