CEN

WORKSHOP

AGREEMENT

CWA 15499-1

February 2006

ICS 03.100.30

English version

Personal Data Protection Audit Framework (EU Directive EC 95/46) - Part I: Baseline Framework

This CEN Workshop Agreement has been drafted and approved by a Workshop of representatives of interested parties, the constitution of which is indicated in the foreword of this Workshop Agreement.

The formal process followed by the Workshop in the development of this Workshop Agreement has been endorsed by the National Members of CEN but neither the National Members of CEN nor the CEN Management Centre can be held accountable for the technical content of this CEN Workshop Agreement or possible conflicts with standards or legislation.

This CEN Workshop Agreement can in no way be held as being an official standard developed by CEN and its Members.

This CEN Workshop Agreement is publicly available as a reference document from the CEN Members National Standard Bodies.

CEN members are the national standards bodies of Austria, Belgium, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland and United Kingdom.

EUROPEAN COMMITTEE FOR STANDARDIZATION
COMITÉ EUROPÉEN DE NORMALISATION
EUROPÄISCHES KOMITEE FÜR NORMUNG

Management Centre: rue de Stassart, 36 B-1050 Brussels

Ref. No.:CWA 15499-1:2006 D/E/F

Contents

Foreword

Managing the protection of personal data is important: such protection is mandatory under the EU Directive (95/46/EC) and national data protection legislation, and, individuals (data subjects) trust that their data is handled in accordance with their expectations. Inappropriate or unauthorised processing of personal data may damage relationships between the data controllers and the data subjects (for example, relationships between customers and their suppliers, employees and their employers and citizens and government institutions).

Since personal data is being processed using more and more complex and interrelated information and communication technologies, the protection of personal data (including security measures) and trust between data subjects and organisations handling their personal data are essential conditions for the conduct of (e-) business and (e-)government. As a result of the number of current and expected transactions and activities carried out online, protection of personal data and trust become more and more important issues.

Organisations will be concerned with whether the personal data they process is handled in accordance with data protection principles and whether the organisation has an adequate and effective Personal Data Protection system in place. Assurance on these matters can be provided by a data protection audit.

A data protection audit helps the organisation to:

- identify non-compliance issues and/or to detect weaknesses in its own data processing management structure;
- maintain compliance with relevant data protection requirements / ensure compliance with relevant data protection requirements.

A data protection audit may also contribute to avoiding breaches of statutory obligations (breaches which may result in sanctions, without excluding other obscure effects for the company's reputation and long term welfare). In addition, for some organisations the data protection audit is an important means of demonstrating compliance with data protection rules (e.g. via a trusted third party opinion and/or a certificate of compliance and/or a letter of comfort). A positive outcome from an audit can be used by an organisation as a marketing tool to gain a business advantage over its competitors.

In 2004, the CEN/ISSS Data Protection and Privacy Workshop compiled an inventory of data protection auditing practices used by businesses throughout the EU and considered whether the process of data protection auditing could benefit from standardization[1]. It was found that, whilst good material is available, there is no baseline audit framework (based on the EU Directive on Data Protection) for organisations that are active in the EU, providing for an efficient approach and enabling comparison of results. The "Personal Data Protection Audit Framework" seeks to provide this baseline audit framework.

1 Inventory of Data Protection Auditing Practices, European Committee for Standardization – Information Society Standardization System, Workshop Data Protection Area B, 2004 (available at www.cenorm.be/isss).

It is CEN/ISSS' aim that the "Personal Data Protection Audit Framework" will help businesses to adhere to the principles of the EU Data Protection Directive and create further awareness of the principles relating to the protection of personal data. As a baseline, it can easily be tailored and used as a means to assess whether a data processing operation meets other data protection requirements (such as national data protection law) as well.

This audit framework is prepared by PricewaterhouseCoopers and Law ID's in close co-operation with the following companies:

- ANEC
- British Standardization Institute
- Commission de la Protection de la Vie Privée in Belgium
- DaimlerChrysler
- Deutsche Telekom
- DLA Piper Rudnick Gray Cary, Belgium
- IMS Health
- Information Commissioner in the UK
- Intel
- Microsoft
- Shell International

The present CWA (CEN Workshop Agreement) has received the support of representatives of a variety of backgrounds. A list of the individuals and organizations which supported the consensus represented by this CEN Workshop Agreement is available from the CEN Management Centre.

The CWA was approved at the Workshop meeting of 1 December 2005 in Paris following its availability during 60 days on CEN's web-site for public comments as well as for final comments by the registered Workshop participants.

This CEN Workshop Agreement is publicly available as a reference document from the National Members of CEN: AENOR, AFNOR, ASRO, BSI, CSNI, CYS, DIN, DS, ELOT, EVS, IBN, IPQ, IST, LVS, LST, MSA, MSZT, NEN, NSAI, ON, PKN, SEE, SIS, SIST, SFS, SN, SNV, SUTN and UNI.