CEN

WORKSHOP

AGREEMENT

CWA 16113

April 2010

ICS 35.020

English version

Personal Data Protection Good Practices

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, Bulgaria, Croatia, 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: Avenue Marnix 17, B-1000 Brussels

Ref. No.:CWA 16113:2010 E

Table of Contents

FOREWORD 8

1 BACKGROUND 9

1.1 General 9

1.2 Target Audience 9

1.3 Relationship to other CWA's 10

2. DATA PROTECTION AND INFORMATION HANDLING COMPLIANCE 13

2.1 General 13

2.2 What is Personal Data? 14

2.3 Notification of Processing to Your National Supervisory 15

Authority 15

2.4 Are you a Data Controller, Processor or Both? 19

3 DATA TRANSFERS ABROAD 22

3.1 General 22

3.2 Contracts 22

3.3 Binding Corporate Rules 23

3.4 International Safe Harbor Privacy Principles 24

4 RIGHTS OF CONSENT & ACCESS 27

4.1 A Data Subject has the Right to Access Data you hold 27

4.2 Information to be given to the Data Subject - The obligation to inform the Data Subject (transparency principle) 28

5 GOOD PRACTICES: DATA LOSS PREVENTION POLICIES & PRACTICES 31

5.1 HOW CAN YOU FULFILL YOUR COMPLIANCE OBLIGATIONS? 31

5.2 Develop A Data Protection/Information Security Policy 31

5.3 Develop an Acceptable Use Policy 33

5.4 Develop a Data Classification & Labeling Policy 34

5.5 Conduct a Privacy Impact Assessment (PIA) 36

5.6 Develop a Data Protection Compliance and Audit Program 37

6. GOOD PRACTICES: HANDLING PERSONALLY IDENTIFIABLE INFORMATION 39

6.1 General 39

6.2 Grounds for processing special categories of personal data 40

6.3 Proportionality 41

6.4 Verify the Quality of Data 42

6.5 Verify that Legitimate Processing (including special categories) is being accomplished 42

6.6 Automated decision making 43

6.7 Retention 44

6.8 Develop a Sub-contracting Contract and Include the Requirements for Data Protection 45

6.9 Selecting a Data Processor 46

6.10 Contracting with a Data Processor 47

6.10.1 General 47

7 GOOD PRACTICES: OPERATIONAL PROTECTION MEASURES 49

7.5 Training and awareness 49

7.6 Process and Procedures 50

7.7 Develop a Incident Handling Policy 50

7.8 Make users aware that Monitoring is done and explain the Goals for Monitoring with respect to Incident Response 51

7.9 Responsibilities of those responsible for Privacy within the Organization 51

7.10 Preventing Data Privacy Incidents 51

APPENDIX A – DEFINITIONS 52

APPENDIX B- REFERENCES 54

APPENDIX C- DATA PROTECTION AUTHORITIES 58

APPENDIX D- DPP CONSORTIUM MEMBERS 59

FOREWORD

This CWA (CEN Workshop Agreement) provides good practice guides to help SMEs comply with the general principles already existing in the Data Protection Directive and where possible and appropriate, the national laws implementing the Directive.

The production of this CWA was formally accepted at the Workshop's kick-off meeting on 2008-03-11.

CWA approval was obtained following an electronic approval process which started on 8 February 2010 and finished on 28 February November 2010.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CEN [and/or CENELEC] shall not be held responsible for identifying any or all such patent rights.

The education sector data protection and privacy best practices developed as part of this effort were adopted in 2008 by the British Educational Communications and Technology Agency, BECTA. They are published at:

http://schools.becta.org.uk/index.php?section=lv&catcode=ss_lv_mis_im03&rid=14734

This CWA has been approved by participants from the following organizations:

Avoncroft Guesthouse (representing the UK B&B's SME community)
FEDMA
ixAssociates Limited
John Borking Consultancy
Mansfield BV
PENSIVE
RAZONA technology
RDE Global
Rhinefield Technology Consultants
The UK Information Commissioner's Office
TNO
TÜV Rheinland Secure IT GmbH

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

Comments or suggestions from the users of the CEN Workshop Agreement are welcome and should be addressed to the CEN-CENELEC Management Centre.

1 Background

1.1 General

In 2004 and 2005 the CEN Workshop on Data Protection and Privacy (WS/DPP) in conducted a research exercise to identify, and produce an inventory, of data protection 'good practices' throughout industry.

Following the good practices outlined in this document, it will help organizations and individuals comply with the general data protection principles set out in Directive 95/46/EC (EU Data Protection Directive). This Directive applies to the processing of personal data and to the free movement of such data. They will help you comply with the National Laws implementing the Directive.

Due to the increasing number of online activities, privacy, data protection and trust issues have become critical for both industry and individuals. Organizations must be able to demonstrate that they have implemented a Data Protection Management System (DPMS) to prove appropriate technology (PETs) and operational protective measures (OPMs) were employed to protect personal data. For SMEs, use of these good practices and the associated CWA DPP audit tools would provide an important means of demonstrating their commitments for compliance with the Directive.

As greater amounts of personal data are being processed, privacy and trust are essential conditions for conducting eBusiness and running eGovernment processes. A breach of privacy can reduce trust and potentially damage relationships between employers and their employees, citizens and government institutions, customers or suppliers. Management commitment to protecting personal data therefore is vital.

1.2 Target Audience

This document is targeted for use by Small to Medium size Enterprises (SMEs) in the European Union. It defines a set of voluntary good practices for Operational Protection Measures and appropriate use of Privacy Enhancing Technologies to help businesses and data managers comply with Directive 95/46/EC. They are intended to generally apply across all Member States, but may need to be supplemented by country specific advice.

Clauses 1-5 provide information to help you understand what is personal data, conditions for its processing, guidance for notification and understanding of the National Data Protection and Privacy Supervisory roles and enforcement powers. The remaining clauses provide good operational and technological practices to help comply with the Directive.

As individuals and organizations, we are responsible for safeguarding privacy and managing information risks for those whose personal data we are entrusted with.

1.3 Relationship to other CWA's

1.3.1 General

This document has relationships to several previous CWA's.

1.3.2 IPSE

The Initiative for Privacy Standardization in Europe (IPSE) in its [2001] report put forward recommendations that could assist business in implementing Directive 95/46/EC. Recommendation 1 was directed at the production of a set of common European voluntary best practices for Data Controllers and Data Processors which has been addressed by this document:

- Personal Data Protection Good Practices

Recommendation 4 considered the possibility of standardization of data protection auditing which has produced:

- Personal Data Protection Audit Framework (CWA 15499-1 and CWA 15499-2)
- Personal Data Protection Self-Assessment Framework

In 2005, the Personal Data Protection Audit Framework was developed. 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. The audit framework is a tool for professional auditors, either internal or external to the organization of the Data Controller and / or Data Processor.

The Self-Assessment Framework translated the Audit Framework into a tool that can be used by organizations to prepare for a personal data protection audit (i.e., to decide whether the organization is indeed ready for an audit).

The 'Self-Assessment framework for managers' provides a set of tools to help measure the level of compliance against basic personal data protection rules and a set of controls. The purpose of this framework is to enable managers to measure their organization's level of compliance with the applicable regulations (taking the European Data Protection Directive (95/46/EC) as the reference law), and if relevant, identify where improvements are necessary and / or desirable. It is intended to provide guidance to the non-expert manager. Of course, the Self-Assessment framework can also be used by experts, for example a privacy officer / data protection officer (either working for a Data Controller or a Data Processor).