CEN

WORKSHOP

AGREEMENT

CWA 16112

April 2010

ICS 35.240.50; 35.240.70

English version

Self-assessment framework for managers

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 16112:2010 D/E/F

Table Of Contents

Foreword

The production of this CWA (CEN Workshop Agreement) specifying a Voluntary Technology Dialogue Framework, 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 2 November 2009 and finished on 30 November 2009.

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.

Together with this CWA a set of templates in the form of questionnaires are provided to facilitate the assessment process and document the findings. These templates are provided in the form of excel spreadsheets and can be downloaded from:

http://www.cen.eu/cen/Sectors/Sectors/ISSS/CEN%20Workshop%20Agreements/Pages/DPPCWA.aspx

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

DELOITTE BELGIUM
DEUTSCHE TELECOM AG
FEDMA
ICRI-K.U-LEUVEN
IQNet/SQS
IxASSOCIATES
John BORKING Consultancy
MANSFIELD B.V
MICROSOFT CORPORATION
PRICE WATERHOUSE COOPERS
RAZONA technology
RDE-Global LLC
SHELL INTERNATIONAL BV
Spanish Data Protection Agency (SDPA)
TNO
TUV RHEINLAND SecureiT GmbH
UK OFFICE OF THE INFORMATION COMMISSIONER
UNIVERSITE PARIS OUEST NANTERRE

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.

Management Summary

Managers are concerned with the interests and responsibilities of developing their business, protecting their organizational assets, and ensuring compliance with applicable laws and regulations. In recent decades, the rapid development of information and communication technologies means that they are now integrated into every aspect of the business, allowing companies and organizations to attract and accept new customers online, manage and store customers' records digitally, and transfer information in real-time and across international borders over the internet to and from the organization's intranet. This new technology-based dimension to operations has introduced new business opportunities but has also introduced new risks in the area of personal data protection (PDP) for companies and organizations.

Managers are responsible for conducting their organization's business legally and protecting their organizations' information assets and will be held liable for any negligence. Acting responsibly requires managers to investigate and understand the risks that their organizations are facing, and take sensible measures to minimize or eliminate identified risks. One such risk is the failure to process personal data in compliance with the PDP. This *self-assessment framework for managers* considers the European Data Protection Directive's data processing requirements, and helps managers to be compliant with the relevant laws and regulations. Moreover, by understanding and embracing their PDP responsibilities, managers can establish good data protection governance and transparent processes and prevent personal data-loss related costs such as reputational damage and loss of business.

The self-assessment framework consists of two parts:

- *The self-assessment process*: explains step-by-step how to carry out a self-assessment. A set of templates in form of questionnaires are provided to facilitate the assessment process and document the findings. Following the tips and recommendations on how to properly conduct cyclic self-assessments can benefit an organization and its business in the long term by establishing good business practices, gaining trust from stakeholders and customers, and ensuring compliance with relevant laws and regulations.
- *The managers' responsibilities*: explains the managerial responsibilities when collecting, processing and disclosing personal data. It aims to help managers understand the personal data processing process and their responsibilities in relation to each phase of the process. By understanding their responsibilities managers are able to identify appropriate measures towards establishing a good PDP practice.

The requirements of the Data Protection Directive are discussed in Section A. Managers are recommended to read this Section before completing the self-assessment questionnaires.

Introduction

Personal data is a valuable asset for individuals, private companies and public organizations. The processing of personal data has become integrated into the routinely daily work of companies of all sizes and business structures. Such data processing has taken on a new dimension with the increased use of (complex) information and communication technologies (ICT), including e-business.

Data processing operations may concern several categories of individuals: customers, citizens, business partners, company employees or suppliers, to name only a few. The implementation of automated business solutions in the course of almost any business activity (from human resources to customer relationship management) increases the opportunities for a more intensive, systematic and multi-dimensional use of data. Data flows between different actors during a business process increase in volume and frequency and in a way that the individuals concerned may not fully control. As a result, the fair use of personal data and the maintenance of trust in the way data are processed, for a number of reasons, becomes a real challenge for any company or government institution.

First, inappropriate or unauthorized use of personal data may damage relationships between organizations and individuals (for example, relationships between customers and their suppliers, employees and their employers and citizens and government institutions). Consideration of privacy and data protection issues is therefore vital in order to gain and maintain the confidence of individuals (Data Subjects).

Furthermore, not only is it in the business interests of organizations to consider data protection and privacy in their business processes, compliance with data protection legislation is mandatory. Processing personal data is subject to various data protection regulations. In addition there are a variety of ‘good’/ ‘best’ practice recommendations aligned to these regulations, including industry standards and company specific personal data protection (PDP) related policies and standards.

In addition, managers must ensure that their data processing operations comply with the regulations applicable in their business environment (including codes and guidelines relevant to the exercise of their activity and sectoral laws) as well as the company’s own business ethics. Although most managers are aware that various laws and rules must be taken into account when processing personal data, they do not know how to interpret and apply such rules. Accordingly, guidance on questions such as:

- What do the rules actually mean for the operations for which my department is responsible?,
- How can these rules be complied with in practice?
- To what extent do we meet the rules / what is the level of compliance? and, “
- What are the risks if we cannot / will not follow such rules?

will hopefully fill a gap in many managers’ understanding of their obligations.

The Self-Assessment Framework for Managers aims to provide clear basic responses to the above questions. In general, this document defines *a process* and *method* that helps managers determine whether basic privacy principles are met within their organization. Regularly performing the self-assessment described herein can support managers to drive forward good privacy practice within their organizations.

The purpose of the guidelines set out in this framework is to provide guidance to the *non-expert manager*[1]. The *Framework* enables the manager to assess his organization's level of compliance with the applicable laws, regulations and (respective) PDP requirements, and if relevant, identify where improvements are necessary and / or desirable.

The position of the self-assessment framework

The nature and the scope of the Personal Data Protection Self-Assessment framework (referred to in this document as the "PDP Self-Assessment Framework" or "Framework") is set out in Clause 1. Please note that this Framework is different from privacy impact assessment tools (PIA) and PDP audit tools. The inter-relationship between these three sets of guidance materials, their scope and their target audiences is summarised in Table 1:

Table 1

Tool	Privacy Impact Assessment (PIA)	PDP Self-Assessment Tools	PDP Audit Tools
Use	PIA tools help to consider the effects / the impact of new initiatives on the privacy of individuals.	PDP Self-Assessment tools help *non-privacy experts* to measure whether processing of personal data is in accordance with the rules of the EU data protection directive.	PDP Audit tools help *auditors* to measure whether processing of personal data is in accordance with the rules of the EU data protection directive.
Objective	To identify and address privacy issues or risks well in advance in order to avoid and prevent costly redesign and adjustment of the program or services at later stage, or even project failure.	To assess the level of compliance with personal data protection rules.	To give assurance (or evaluate) whether personal data is handled in accordance with data protection rules and whether the organisation has an adequate and effective PDP system in place.
Reference	Privacy / Data Protection Principles based on applicable PDP related laws and regulations.	Basic PDP rules and controls framework.	Requirements framework.
When	The PIA should be used in the planning phase or in case of major changes in the existing data processing operation.	Self-assessments can be used whenever the company/manager wants to measure compliance.	Audits can be carried out whenever the assigner (i.e. a manager, business partner or sub-contractor of the data controller) wants (independent) assurance regarding the level of compliance.
Key user	Team of experts (including a privacy expert) who carry out the PIA on request e.g. the party that initiates and undertakes a project.	Manager or person / team acting on behalf of the manager who carries out the self-assessment.	Auditor / independent party who has no interest in the outcome of the audit.

[1] i.e. An individual who is not expert in data protection and privacy matters and the associated legislation. Yet, other users, including privacy experts, can also use the tool. Potential users of this Framework can therefore be company in-house privacy officers / data protection officers and members of the employment councils. Parts of the tool may also be relevant for IT professionals (e.g. the part on security) and staff involved in procurement (e.g. the part of Data Processors).

Abbreviations

BCR	Binding Corporate Rules
CAAT	Computer Assisted Audit Tools
DP	Data Protection
DPD	Data Protection Directive
EC	European Commission
EU	European Union
PDP	Personal Data Protection
PET	Privacy Enhancing Technologies
TBDF	Trans Border Data Flows

Introduction to the self-assessment framework

Background

As a manager, you are responsible for ensuring that your business operations comply with all applicable laws, regulations and codes of practice. You understand that a number of the business activities carried out by your company involve the use, storage or communication of data about individuals. You are also aware that such personal data require protection and that there are limits to the ways in which your company is permitted to process them. This Self-Assessment Framework will help you to understand what the rules and limits on the processing of personal data mean in practice and determine whether your company has implemented structures and processes to meet its obligations with regard to the processing of personal data.

This Framework provides hands-on guidance as to how to carry out the data protection self-assessment. Firstly, this document can be considered as a practical tool to be used “on the spot” whenever you wish to measure the consistency of your business practices with basic data protection rules. Secondly, it will contribute to identifying specific gaps in the way you currently protect personal data within your business. Finally, it will improve your understanding around the impact of PDP related regulations on the operations for which you are responsible.

The purpose of performing a ***Self-Assessment*** is primarily to assess your business’ level of compliance with privacy rules. After performing a Self-Assessment the (potential) gaps within your business in relation to data protection and privacy will be clear.

Drivers for conducting a Self-Assessment can be:

- The desire/intention to gain a better insight into the company’s data handling practices and its level of compliance with basic privacy rules.
- The obligation to meet a mandatory internal requirement (e.g. where the organization requires managers to report on privacy compliance).
- The need to assess whether the organization is ready for a privacy audit.

Indirect motives for undertaking this Self-Assessment exercise can be:

- The desire to enhance the confidence of business stakeholders (customers, employees, etc.) in the way privacy and personal data are protected within a company.
- The desire to ensure long-term privacy compliance as a business goal and by adopting a holistic approach.
- The desire to integrate privacy and data protection into the company’s vision and values.

Benefits of performing a Self-Assessment may include:

- Enhancing the company’s knowledge of the existing practices and procedures that it has put in place to protect personal data.
- Enhancing the privacy awareness of staff involved in processing personal data.