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.
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 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
CWA 16113:2010 (E)

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:


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).
Recommendation 6 concerned the establishment of a coordination and early-warning system for new developments in technology to assist data protection commissioners and business which has produced:

- The Voluntary Technology Dialogue System

Ensuring new products, technologies and services comply with the relevant Data Protection and Privacy laws as transposed in all EU Member States can be a challenging task for industry. In addition, regulators find themselves somewhat unaware of potential new technologies likely to reach the market in the near future. In an effort to help both industry and regulators overcome these hurdles, it is a voluntary systematic process enabling companies of all sizes (small and medium sized enterprises through to multi national corporations) to work more closely with regulators during the development cycle of new products.

European regulators welcomed the opportunity to be briefed on emerging technology roadmaps via the dialogue system to assist meeting their obligations to provide “better regulation”.

This voluntary technology framework incorporates lead times, documentation requirements, escalation procedures, confidentiality practices and the dialogue process itself.

1.3.4 Inventory of Data Protection Auditing Practices – CWA 15262

In 2004, an inventory of data protection auditing practices used by businesses throughout the EU was carried out and considered whether the process of data protection auditing could benefit from standardization.

In addition to audit frameworks and quick scans, compliance questionnaires were integrated in the Self-Assessment Framework.

1.3.5 Analysis of Privacy Protection Technologies – CWA 15263

Privacy Protection Technologies are considered as useful tools in enhancing the privacy of the user, which could be implemented in hardware and/or software have been identified in this report.

1.3.6 Standard form contract to assist compliance with obligations imposed by article 17 of the Data Protection Directive 95/46/EC (and implementation guide) - CWA 15292

Contracts have long been considered useful tools in achieving data protection compliance. The achievement of a form of contract accepted by all sides of an industry, containing generic phraseology that can be adapted according to the individual circumstances, is a most valuable form of business standard for trade. There is clearly

---

1 It was found that there was no baseline audit framework (based on the EU DP Directive) for organisations that are active in the EU, providing for an efficient approach and enabling comparison of results. The “PDP Audit Framework” seeks to provide this baseline audit framework.
no need to re-invent the wheel every time a contract is drafted, and indeed there are standard contracts for a variety of purposes.

In 2005, generic contract clauses (a standard form contract for contractual relations in common areas of professional and other services, reflecting the requirements of Article 17 of Directive 95/46 for use within the EEA) and an implementation guide were developed.
2. Data Protection and Information Handling Compliance

2.1 General

Protecting personal and sensitive information is mandatory and enforced by Directive 95/46 of the European Parliament, its supplements and Local Laws. Fines and custodial sentences may be imposed as a result of serious data protection breaches. The loss of privacy, basic freedoms and human rights of the concerned individual(s) are at the foundation of these laws.

At a very high level, the basic principles of the Directive include the following regarding protected data:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate and up to date
- Not kept for longer than is necessary
- Processed in line with individual’s rights
- Secure in processing, storage and transfer
- Not transferred to other countries without an adequate level of protection

Everyone has the right to privacy and individuals with special needs, young persons and those at risk, deserve even more protection. Businesses and Government have the responsibility to protect the data entrusted to them, not just as an obligation to the law, but as a personal pledge to each individual.

Each Member State has specific legislation that implements and supplements the Directive. On a national level, the Directive is translated into laws and regulations designed to protect the rights of individual’s in respect to their personal information. It places the emphasis on the rights of the individual over the rights of anyone collecting, storing or using personal information for almost any purpose.

The Directive and information rights in general are championed by each country’s official Data Protection Supervisory Authority. The Directive itself and your country’s implementation of it can be found at the links provided in Appendix C.
2.2 What is Personal Data?

2.2.1 General

The Directive states that- Personal data is any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to their physical, physiological, mental, economic, cultural or social identity.

There are different ways in which an individual can be considered ‘identifiable’. Some data is uniquely identifying on its own (e.g., DNA, National ID, etc.) others only in association (e.g., a street address with the name of the resident). You must also consider the realities of a digital identity (those typically stored in a cookie, a digital signature or as any type of digital object that is unique to an individual or directly linked to an individual). Computer processes frequently act on the behalf of an individual and assume their identity in legal ways.

2.2.2 “Digital ME”

Your personal data exists in many digital forms and is included in browsers in the form of certificates. Mobile phones are (generally speaking) uniquely identifiable to an individual, your home, appliances and even your clothing may include technology (e.g., Smart Metering, the Internet of Things or RFID) may represent your identity; and social networking sites reflect your identity and personal information in great detail. “Digital ME” includes:

- Digital information stored in databases, video (including CCTV), pictures
- Documents, files, notebooks, pictures, invoices, medical records
- RFID, ID Cards, Passports
- Cookies, flash objects, eID middleware
- Biometric identifiers (e.g., fingerprints, DNA)
- Data forming part of a relevant filing system
- Data forming part of an accessible record
- Data recorded by a public authority

“Digital ME” refers to the digital representation of your personal or organization’s identity.

The personal information you post online, combined with data that depicts your actions and interactions with other people, can create a rich profile of your interests.
and activities. Personal Identifiable Information (PII) published on social network sites for example, can be used by third parties for a wide variety of purposes, including marketing, debt collection and investigations. Major risks such as identity theft, financial loss, loss of business or employment opportunities as well as, physical harm can result from this electronically omni-present data.

All of the above examples of personal data are governed by Directive 95/46EC. The Directive mandates that appropriate protective measures (i.e., OPMs and PETs) be implemented for processing of this data by automatic means (computers) and non-automated processing (within a 'filing system').

Today's search engines have the ability to combine your dispersed data (personal data you post in different systems) in ways that you originally had not intended. Once you make this information available, the use of it is in the hands of the Public and generally speaking, no longer in your control.

### 2.3 Notification of Processing to Your National Supervisory Authority

#### 2.3.1 General

Notification is the process by which a Data Controller informs the National Authority of certain details about their processing of personal information. These details are used by the Authority to make an entry describing the processing in the register of Data Controllers which is available to the public for inspection.

Notification is a statutory requirement in most Member States and every organization that processes personal information must notify their National Data Protection Supervisory Authority unless they are exempt or do not process data of the type required for notification.

**NOTE:**
The Article 29 Working Party has published a guide on notification requirements. This guide is intended to summarize the basics of the notification system in each country with a view to supporting Data Controllers in complying with the relevant requirements on “notification requirements”


Notification serves the interests of individuals by helping them understand how personal information is being processed by Data Controllers.
Relevant articles: DPD 95/46/EC art. 18, 19, 20, 21

Explanation of your responsibilities / Obligations for Administrative requirements include:

1. Prior checking means that the National Data Protection Supervisory Authority is informed by the Data Controller about the intention to start a certain data processing operation and is given the opportunity to conduct a prior check.

2. In most countries (there are exceptions) notifying means that the Data Controller provides the National Data Protection Supervisory Authority with several details about the data processing operation. In practice, Data Controllers often complete a form (either hardcopy or an electronic version) and send / submit this form to the national data protection authority.

Notification should be completed before you start collecting personal data or starting processing activities. It is recommended to keep copies of all communications (including the information that has been notified) sent to and received from the National Data Protection Supervisory Authority.

Organizations should appoint a person who periodically checks whether the notified information is still complete, accurate and up-to-date, or whether the grounds for exemption still apply / are still valid.

- The principal purpose of having notification and the public register is transparency and openness. It is a basic principle of data protection that the Public should know who is carrying out the processing of personal information as well as, other details about the processing. Notification, therefore, serves the interests of individuals by helping them understand how personal information is being processed by Data Controllers.

2.3.2 Types of Personal Data that may Require Notification

Typically, notification to the Supervisory Authority will include details of the types of information in which you will be the Data Controller or Data Processor. Supervisory Authority’s may have different categories and groupings of types of data that you can choose to describe your processing requirements. If you intend to collect, process or store data in any of the following general categories (not all inclusive), you need to register with your Supervisory Authority:

- Address, home contact details, date of birth, personnel/payroll number, PPS number, salary and pension details, annual and sick leave records, details of next of kin, current and previous employment records, CV / qualifications, bank details

- Accounting and auditing. The provision of accounting and related services, the provision of an audit where such an audit is required by statute

- Administration of justice-Internal administration and management of courts of law or tribunals and discharge of court business
Ja, ik bestel

__ ex. CWA 16113:2010 en Personal Data Protection Good Practices € 53.00

Wilt u deze norm in PDF-formaat? Deze bestelt u eenvoudig via www.nen.nl/normshop

Gratis e-mailnieuwsbrieven
Wilt u op de hoogte blijven van de laatste ontwikkelingen op het gebied van normen, normalisatie en regelgeving? Neem dan een gratis abonnement op een van onze e-mailnieuwsbrieven, www.nen.nl/nieuwsbrieven

Gegevens

Bedrijf / Instelling
T.a.v. O M O V
E-mail
Klantnummer NEN
Uw ordernummer BTW nummer
Postbus / Adres
Postcode Plaats
Telefoon Fax
Factuuradres (indien dit afwijkt van bovenstaand adres)
Postbus / Adres
Postcode Plaats
Datum Handtekening

NEN Standards Products & Services
Postbus 5059
2600 GB Delft
Vlinderweg 6
2623 AX Delft
T (015) 2 690 390
F (015) 2 690 271
www.nen.nl/normshop

Retourneren
Fax: 015 2 690 271
E-mail: klantenservice@nen.nl
Post: NEN Standards Products & Services, t.a.v. afdeling KIantenservice Antwoordnummer 10214, 2600 WB Delft (geen postzegel nodig).

Voorwaarden
• De prijzen zijn geldig tot 31 december 2018, tenzij anders aangegeven.
• Alle prijzen zijn excl. btw, verzend- en handelingskosten en onder voorbehoud bij o.m. ISO- en IEC-normen.
• Bestelt u via de normshop een pdf, dan betaalt u geen handeling en verzendkosten.
• Meer informatie: telefoon 015 2 690 391, dagelijks van 8.30 tot 17.00 uur.
• Wijzigingen en typefouten in teksten en prijsinformatie voorbehouden.
• U kunt onze algemene voorwaarden terugvinden op: www.nen.nl/leveringsvoorwaarden.

LEREN, WERKEN EN GROEIEN MET NEN