



Personal Data Protection Certifications

Bruxelles, September 19th 2017



UNINFO

Speaker's introduction

Fabio GUASCONI

- UNINFO (Italian standardization body for ICT) board of directors
- President UNINFO CT 510 - ISO/IEC JTC1 SC27 mirror
- CLUSIT board of directors
- SBS expert
- CISA, CISM, PCI-QSA, ITIL, ISFS, Lead Auditor 27001 & 9001
- Partner and co-founder @ **Bl4ckswan** S.r.l

Agenda

GDPR and certification

- What is required in articles 40 to 43
- How are certifications referred to in GDPR

Data protection certifications market

- Certifications market history & analysis
- Current main certification schemes
- Existing and future standards

National initiatives

- Italian ISDP 10003:2015

Conclusions

What is required in articles 40 to 43

Articles 40 & 41 – Codes of conduct

- ✓ Prepared by associations and other bodies representing categories of controllers or processors to specify the application of GDPR
- ✓ Subject to supervisory authority opinion
- ✓ Compliance can be monitored by bodies with appropriate level of expertise and accredited by the supervisory authority

Articles 42 & 43 – Certification

- ✓ Issued by certification bodies or supervisory authority on the basis of criteria approved by that competent supervisory authority / board
- ✓ Voluntarily usable by controllers and processors
- ✓ With maximum 3 years of validity, focussing on processing operations*
- ✓ Certification bodies must be accredited by the competent supervisory authority or by the national accreditation body in accordance with EN-ISO/IEC 17065/2012 and with the additional requirements established by the supervisory authority

* Processes and services are referenced by recital 100

How are certifications referred to in GDPR

Code of conducts or certification mechanisms are selectively referred to as: **“element by which to demonstrate compliance with the obligations / requirements”** expressed within GDPR articles.

Key references are found in the following articles:

	Code of conduct Art.40	Certification Art.42
Art.24 Responsibility of the controller	✓	✓
Art.25 Data protection by design and by default		✓
Art.28 Processor	✓	✓
Art.32 Security of processing	✓	✓

Certifications market history & analysis



Source: CRISP workshop September 30th 2016

Current main certification schemes

Quick fact sheets



Privacy Mark

~ 21.000 certificates
est. 1998, Japan
PIMS



Label CNIL

~ 90 certificates
est. 2011, France
Processes



EuroPriSe

~ 70 certificates
est. 2008, Germany
PIMS



ePrivacyseal

~ 100 certificates
est. 2011, Germany
Products and services

Existing and future standards

JIS 15001:2006, Personal Information Protection Management System requirements

- Protection of rights and interests of individuals in business PII processings
- PDCA organized management system
- Personal Information Protection Policy
- Specification of personal information (registry)
- Risk analysis and recognition (in each relevant aspect)
- Personal Information Protection Manager
- Procedures for state of emergency
- **Principles on acquisition, use and provision** (including notice, consent)
- **Rights concerning personal information** (modifying, erasing ...)
- Education of employees
- **Not directly related with GDPR or HLS**



Existing and future standards

BS 10012:2017, Specification for a personal information management system

- Recently revised in line with the GDPR, **cross references in each paragraph**
- Management system using ISO HLS
- PIMS policy including data protection principles
- Data inventory and data flow analysis process
- Data protection impact and risk assessment processes providing inputs for treatment and related with PbD
- DPO and other managerial responsibility specification
- Record of privacy notices and link to relevant personal information
- Specification of security measures and management of security breaches
- Exercise of rights from natural persons (including "to be forgotten" and "portability")
- **State-of-the-art work but not certifiable**



Existing and future standards

ISO/IEC 27552, Enhancement to ISO/IEC 27001 for privacy management

- Work in progress (2nd WD), completion planned for April 2019
- Not stand-alone document, following ISO/IEC 27009 setup
- PIMS approach recalled
- Strong focus on controls
- Still too early to be evaluated

Alan SHIPMAN will tell us more in a few minutes



National initiatives

Italian ISDP 10003:2015, international system for personal data protection

- Proprietary scheme endorsed by Accredia **but not by the national DPA**
- DPO responsibility specification
- Privacy manual (including registry and responsibility attributions)
- Documentation requirements (including DPIA and nationally required documents)
- Processing principles including GDPR
- Annex with 57 mandatory control objectives
- **High-level, poorly defined management system**



Conclusions

- 1** Several data protection certification / seal / mark initiatives are under way and more will randomly follow.
- 2** Their average linkability to GDPR is not high but will increase. Many would nevertheless still lack necessary quality.
- 3** Coordinated European initiatives aimed at producing something on the topic are still missing and should be stimulated.

Contacts

UNINFO

<http://www.uninfo.it/>

uninfo@uninfo.it

Corso Trento 13 - 10129 Torino

Tel. +39 011501027 - Fax +39 011501837

Fabio Guasconi

fabio.guasconi@bl4ckswan.com

