Panoramica delle norme tecniche nazionali e internazionali legate al GDPR

Security Summit Milano
15 marzo 2018

UNINFO

Speaker

Fabio GUASCONI

- Direttivo UNINFO
- Presidente UNINFO CT 510 - Sicurezza
- Direttivo CLUSIT
- Esperto SBS
- CISA, CISM, PCI-QSA, ITIL, ISFS, Lead Auditor 27001 & 9001
- Partner e co-fondatore @ Bl4ckSwan

Agenda


GDPR
Enti di normazione coinvolti
Linee guida
GDPR e certificazione
Certificazione delle organizzazioni
Certificazione delle persone
Conclusioni

Enti di normazione coinvolti

ISO/IEC JTC 1/SC 27/ WG 5 “Identity management and privacy technologies”

CEN/CLC/JTC 8 “Privacy management in products and services”

CEN/CLC/JTC 13 “Cybersecurity and data protection”

ETSI TC Cyber

UNI/CT 510/GL 05 “Tecnologie e tecniche per la protezione della privacy e dei dati personali”

CEN ed ETSI

Faticosamente costituito dopo essere stato un JWG e un TC, nel CEN JTC 8 sono finalmente stati concordati i seguenti working items per i quali si sono avviati formalmente i lavori a dicembre 2017:

- **EN Privacy management in products and services**
- **EN TR Video Surveillance**
- **EN TR Access control**

Il TC Cyber di ETSI sta invece lavorando su:

- **TR 103 370 Practical introductory guide to privacy (stable draft)**
- **TS 103 485 Privacy assurance and verification (early draft)**
- **TS 103 458 Application of ABE* for data protection on smart devices, cloud and mobile services (final draft)**

* Application Based Encryption

ISO/IEC 29100 - Generalità

Framework per la protezione dei dati personali trattati con sistemi informativi

- Definizione di termini (**vocabolario**) condivisi per il trattamento delle PII
- Individuazione di **attori e ruoli** per la gestione dei PII
- Analisi delle **interazioni** tra attori in scenari diversi di trattamento delle PII
- **Classificazione** delle PII
  - Considerazioni su metadati e PII non richieste
  - Tecniche di anonimizzazione o associazione a pseudonimi
- **Gestione dei rischi** relativi alla privacy
- **Misure di sicurezza** per far fronte ai rischi individuati
- **Privacy policy**

Liberamente disponibile in inglese e a pagamento in italiano

ISO/IEC 29134:2017 - Generalità

Metodologia per condurre un **Privacy Impact Assessment** funzionale a:

- **identificare rischi** relativi alla privacy e responsabilità collegate
- fornire input per la progettazione di sistemi ("**privacy by design**")
- riesaminare l'impatto sulla protezione delle PII di un **sistema nuovo oppure soggetto a modifiche** significative
- **allocare risorse** per il contenimento di impatti sulla privacy
- **fornire informazioni** su ambiti in cui la protezione dei dati personali è un tema chiave
- **fornire evidenza di conformità** dove questa è richiesta
- **fornire evidenza** ai PII principal **delle misure di protezione** presenti sul trattamento delle loro PII

Linee Guida: ISO/IEC 29134 – Privacy Risks

Privacy risk (29100): **effect of uncertainty on privacy**

Esempi principali:

- **Unauthorized access to PII** (loss of confidentiality)
- **Unauthorized modification of the PII** (loss of integrity)
- **Loss, theft or unauthorized removal of the PII** (loss of availability)

Altri esempi:

- Excessive collection of PII
- Unauthorized or inappropriate linking of PII
- Insufficient information concerning the purpose for processing the PII
- Failure to consider the rights of the PII principal
- Processing of PII without the knowledge or consent of the PII principal
- Sharing or re-purposing PII with third parties without the explicit informed consent of the PII principal.

Linee Guida: ISO/IEC 29151:2017

Catalogo di **controlli per la protezione dei dati personali** pensato per mitigare i rischi relativi alla privacy (c.d. "privacy risks").

Recepisce completamente i principi della ISO/IEC 29100 ed è calata nel framework della ISO/IEC 27002, risultando compatibile con la ISO/IEC 27001.

Aggiunge:

- **Implementation guidance for the protection of PII**
- **Other information for the protection of PII**

Linee Guida: ISO/IEC 29151 – Controlli Aggiunti

Policies for the protection of PII	Use, retention and disclosure limitation	Secure erasure of temporary files	PII disclosure notification	Recording of PII disclosures
Disclosure of sub-contracted PII processing	Privacy notice	Dissemination of privacy program information	PII principal access	Redress and participation
Complaint management	Privacy risk assessment	Privacy requirement for contractors and service providers	Privacy monitoring and auditing	PII protection awareness and training
	PII protection reporting	Continuous Improvement of PII management systems	Cross border data transfer restrictions in certain jurisdictions	

Cosa viene richiesto negli articoli 40-43

Articoli 40 & 41 – Codici di condotta

- ✓ Pensati come strumenti per contribuire all'adeguata applicazione del Regolamento in settori specifici o a soggetti di dimensioni uniformi
- ✓ Preparati da associazioni e altri organismi rappresentanti le categorie di titolari del trattamento o responsabili del trattamento
- ✓ Soggetti all'opinione dell'autorità di controllo competente che esprime un parere della conformità al Regolamento e, in caso positivo, li inoltra al Comitato
- ✓ Il Comitato raccoglie in un registro tutti i codici di condotta, le modifiche e le proroghe approvati e li rende pubblici mediante mezzi appropriati
- ✓ Il controllo della conformità può essere effettuato da un organismo in possesso del livello adeguato di competenze riguardo al contenuto del codice e del necessario accreditamento a tal fine dell'autorità di controllo competente

Cosa viene richiesto negli articoli 40-43

Articoli 42 & 43 – Certificazione

- ✓ Rilasciata da organismi di certificazione o dall'autorità di controllo competente sulla base di criteri approvati dall'autorità di controllo competente o dal Comitato
- ✓ Utilizzabile volontariamente da titolari e responsabili
- ✓ Con validità massima di 3 anni
- ✓ Inerente alle attività di trattamento*
- ✓ Il Comitato raccoglie in un registro tutti i meccanismi di certificazione e i sigilli e i marchi di protezione dei dati e li rende pubblici con qualsiasi mezzo appropriato
- ✓ Gli organismi di certificazione devono essere accreditati dall'autorità di controllo competente o dall'ente di accreditamento nazionale conformemente alla norma ISO/IEC 17065:2012 e ai requisiti aggiuntivi stabiliti dall'autorità di controllo competente

* Processi e servizi sono referenziati nel considerando 100

Come sono referenziate le certificazioni

I codici di condotta o i meccanismi di certificazione sono selettivamente referenziati come: **“elementi per dimostrare il rispetto degli obblighi / la conformità ai requisiti”** espresso negli articoli del Regolamento.

Si possono trovare riferimenti agli articoli principalmente in:

	Codici di condotta Art.40	Certificazione Art.42
Art.24 Responsabilità del titolare del trattamento	✓	✓
Art.25 Protezione dei dati "by design" e "by default"		✓
Art.28 Responsabile del trattamento	✓	✓
Art.32 Sicurezza del trattamento	✓	✓

WP 29 sull'accreditamento

Draft (documento WP 261) del 6 febbraio 2018 che fornisce qualche chiarimento in merito:

- alla conferma dell'uso della **ISO/IEC 17065** come schema di riferimento
- alle possibilità per ogni Paese di avere **l'Autorità**, l'**ente di accreditamento** o **entrambe** coinvolte nello schema
- alla necessità di aderire ai **requisiti aggiuntivi** fissati dall'Autorità anche per gli enti di certificazioni già accreditati rispetto alla ISO/IEC 17065

E' atteso nella versione finale un annex con linee guida per la definizione di requisiti aggiuntivi …

Norme esistenti e future

JIS 15001:2006, Personal Information Protection Management System requirements ("PIPMS"?)

- Protezione di diritti e interessi delle persone nei trattamenti di PII per business
- Sistema di gestione orientato al PDCA
- Personal Information Protection Policy
- Specifica delle informazioni personali (registro)
- Analisi del rischio e ricognizione (in ogni aspetto di rilievo)
- Personal Information Protection Manager
- Procedure per lo stato di emergenza
- **Principi su acquisizione, uso e fornitura** (incluse informative e consenso)
- **Diritti relative alle PII** (modifica, cancellazione …)
- Formazione del personale

Norme esistenti e future

ISDP 10003:2015, international system for personal data protection

- Schema proprietario accreditato da Accredia
- Definizione delle responsabilità del DPO
- Manuale della privacy (inclusive di registro e attribuzione delle responsabilità)
- Requisiti documentali (inclusive della DPIA e documenti richiesti a livello nazionale)
- Principi per il trattamento che riprendono il GDPR
- Appendice con 57 obiettivi di controllo obbligatori

Norme esistenti e future

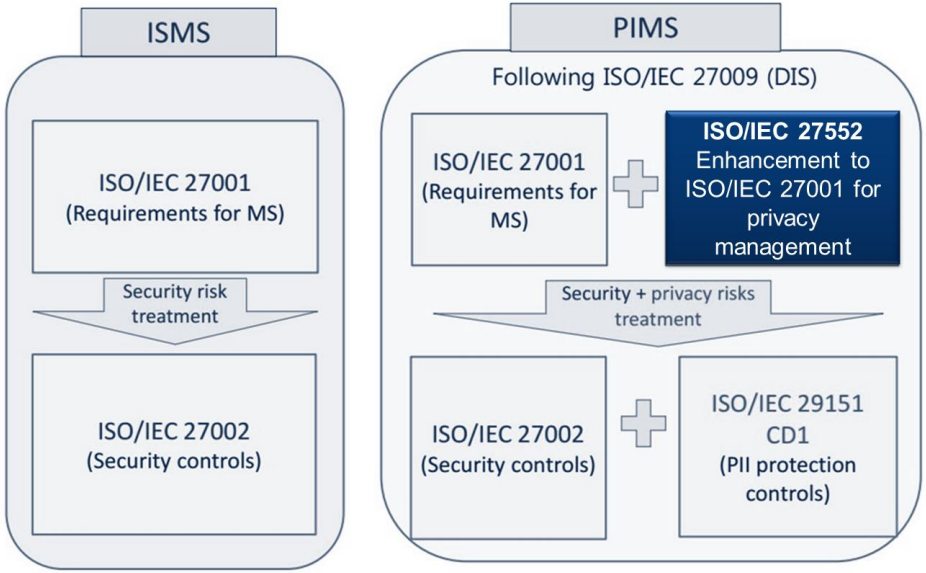
BS 10012:2017, Specification for a personal information management system (PIMS)

- Recentemente revisionata per allineamento con il GDPR, **con riferimenti incrociati in ogni paragrafo**
- Sistema di gestione allineato ad HLS di ISO
- PIMS policy inclusive dei principi per la protezione dei dati
- Processi di DPIA e risk assessment che forniscono input per il trattamento e sono collegati con la PbD
- Inventario dei dati e processo di analisi dei flussi
- Definizione del DPO e di altre responsabilità manageriali
- Registrazione delle informative e collegamento ai dati personali relativi
- Specifica delle misure di sicurezza e gestione delle violazioni
- Esercizio dei diritti (inclusi oblio e portabilità)

Norme esistenti e future

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

- Norma in lavorazione (1st CD) con completamento previsto per aprile 2019
- Documento non autoconsistente che segue le indicazioni della ISO/IEC 27009
- Richiamo dell'approccio verso un PIMS
- Forte attenzione dedicate ai controlli
- Partecipazione attiva del WP 29 e di diverse autorità europee (FR, IT in primis)



Standard esistenti e futuri

Il 18 ottobre 2017 sono stati avviati i lavoro per una Prassi di Riferimento UNI, sponsorizzata da AIP, che definirà le "**Linee guida per la gestione dei dati personali in ambito ICT secondo il Regolamento EU 679/2016 (GDPR)**"

Lo scopo della prassi di riferimento sarà quello di fornire le linee guida per la definizione ed attuazione dei processi afferenti al trattamento dei dati personali, mediante strumenti elettronici (ICT), secondo il Regolamento Europeo 679/2016 (GDPR) e la normativa vigente.

Il 16 gennaio è stata proposta una "**parte 2**" che definisse dei requisiti certificabili sulla stessa materia, con particolare attenzione per le PMI.

La data di rilascio prevista per entrambe le parti prevista è 1 mese prima di quella di applicabilità del Regolamento.

Prassi di Riferimento UNI – parte 2

La parte 2, che mira a inserirsi nei descritti meccanismi degli artt.42 e 43, è intitolata "**Requisiti per la protezione dei dati personali in ambito ICT**" e contiene attualmente i seguenti punti principali:

0 Introduzione
1 Scopo
2 Riferimenti normativi
3 Termini, definizioni e abbreviazioni

4 PIANIFICAZIONE
4.1 Comprendere l'organizzazione e il suo contesto
4.2 Ambito della protezione dei dati personali
4.3 Politica per la protezione dei dati personali
4.4 Ruoli e responsabilità
4.5 Gestione del rischio
4.6 Pianificazione delle modifiche

5 ATTIVITÀ OPERATIVE
5.1 Informative e consensi
5.2 Aggiornamento delle posizioni
5.3 Protezione dei dati personali
5.3.1 Minimizzazione dei dati
5.3.2 Conservazione e cancellazione dei dati
5.3.3 Attuazione e mantenimento delle misure di sicurezza
5.3.4 Gestione delle violazioni dei dati personali
5.4 Richieste di esercizio dei diritti degli interessati
5.5 Formazione e consapevolezza

6 CONTROLLO
6.1 Audit interno
6.2 Relazione periodica
6.3 Non conformità ed azioni correttive

Certificazione delle persone

Gli articoli 42 e 43 sono applicabili anche alle certificazioni delle persone?

Il "common understanding" attuale propende verso una risposta negativa ma non esiste una risposta ufficiale. Nel frattempo il Garante ha rilasciato il seguente comunicato congiuntamente con Accredia il 18/07/2017:

Regolamento Ue e certificazione in materia di dati personali

ACCREDIA e il Garante per la protezione dei dati personali ritengono necessario sottolineare - al fine di indirizzare correttamente le attività svolte dai soggetti a vario titolo interessati in questo ambito - che al momento le certificazioni di persone, nonché quelle emesse in materia di privacy o data protection eventualmente rilasciate in Italia, sebbene possano costituire una garanzia e atto di diligenza verso le parti interessate dell'adozione volontaria di un sistema di analisi e controllo dei principi e delle norme di riferimento, a legislazione vigente non possono definirsi "conformi agli artt. 42 e 43 del regolamento 2016/679", poiché devono ancora essere determinati i "requisiti aggiuntivi" ai fini dell'accreditamento degli organismi di certificazione e i criteri specifici di certificazione.

Certificazione delle persone

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

ESQUEMA DE LA AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS DE CERTIFICACIÓN DE DELEGADOS DE PROTECCIÓN DE DATOS (ESQUEMA AEPD-DPD).

Pubblicato il 10 luglio 2017 indica:

- ✓ Profilo del DPO
- ✓ Competenze richieste
- ✓ Prerequisiti (esperienza e formazione in misura variabile da 5+0 a 0+180 ore)
- ✓ Codice etico
- ✓ Modalità di valutazione (150 domande su 3 domini, normativa – 50%, gestione dei rischi – 30% e tecniche per la protezione dei dati – 20%)
- ✓ Criteri per la certificazione e il mantenimento (3 anni con CPE)

UNINFO

Certificazione delle persone

Norma **UNI 11697** pubblicata il 30 novembre 2017 sui **Profili professionali relativi al trattamento e alla protezione dei dati personali** e basata su e-CF 3.0

DPO (completamente allineato al Regolamento)

Manager privacy

Soggetti con un elevatissimo livello di conoscenze, abilità e competenze in uno specifico contesto organizzativo (sia esso un'area funzionale dell'organizzazione sia il settore di appartenenza della stessa) per garantire l'adozione di idonee misure organizzative nel trattamento di dati personali.

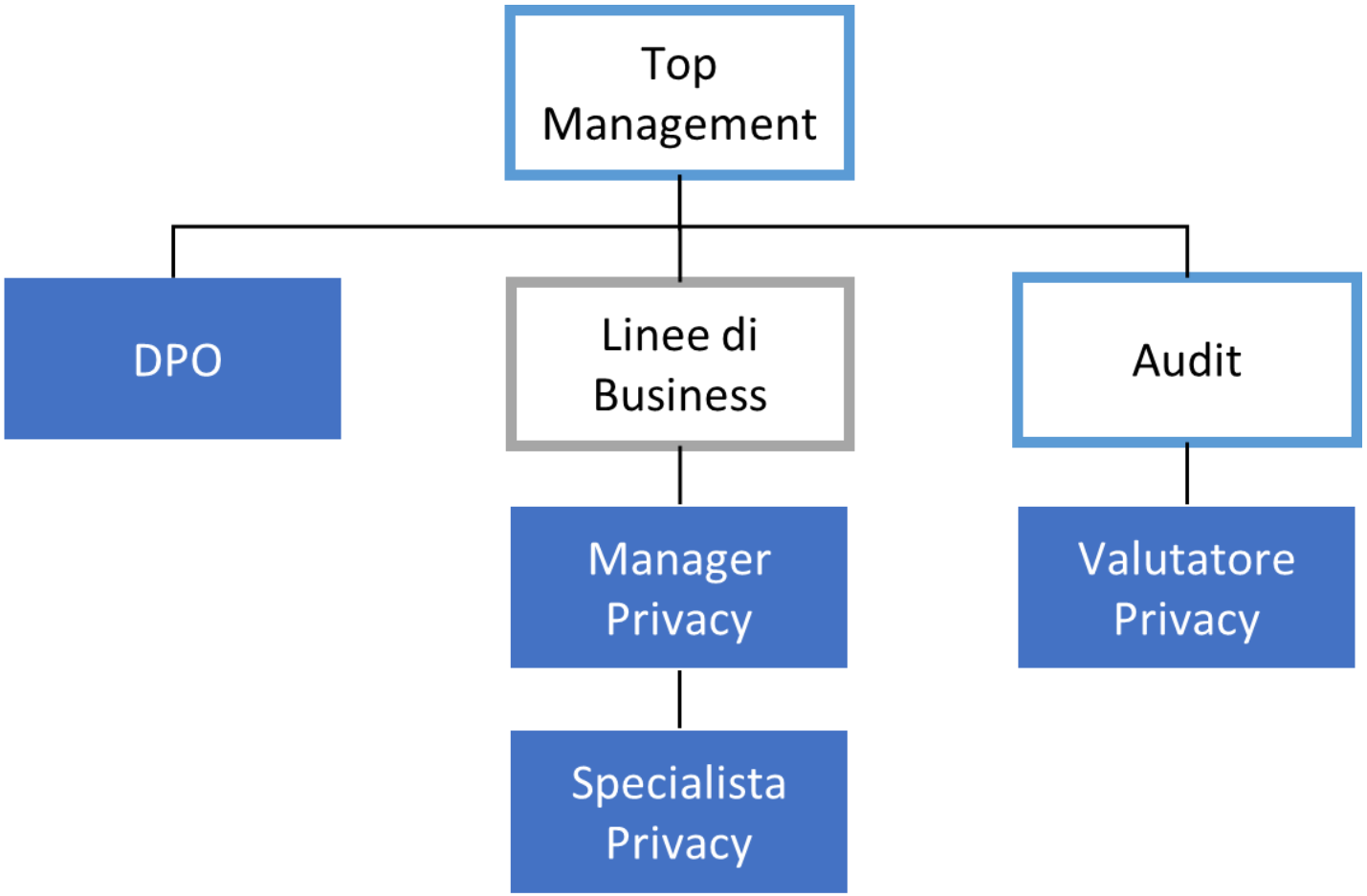
Specialista privacy

Soggetti che supportano il Responsabile per la protezione dei dati personali e/o il Manager privacy nel mettere a punto le idonee misure tecniche e organizzative ai fini del trattamento di dati personali.

Valutatore privacy

Soggetti indipendenti con conoscenze e competenze nel settore informatico/tecnologico e di natura giuridica / organizzativa che conducono attività del trattamento e della protezione dei dati personali che possono comunque avvalersi di specialisti in entrambi gli ambiti per effettuare attività di audit.

Certificazione delle persone



Certificazione delle persone

Livello	Titolo di studio	Formazione specifica	Esperienza lavorativa
Responsabile protezione dati	Laurea	80 ore	6 anni (4 manageriali)
Manager privacy	Laurea	60 ore	6 anni (3 manageriali)
Specialista privacy	Diploma	24 ore	4 anni
Valutatore privacy	Diploma	40 ore	6 anni (3 audit)

Schema di certificazione Accredia

Il 12 febbraio 2018, Accredia ha pubblicato le Disposizioni in materia di certificazione e accreditamento per la conformità alla norma UNI 11697:2017, che uniformano rispetto a tutti gli enti di certificazione:

- i requisiti di competenza degli esaminatori e dei candidati
- i meccanismi di conseguimento multiplo, transizione e rinnovo
- le seguenti modalità di svolgimento dell'esame oltre all'esame del CV

RPD/DPO	Prova scritta da 40 domande a risposta multipla e 3 casi studio Esame orale da almeno 40 minuti
Manager privacy	Prova scritta da 35 domande a risposta multipla e 3 casi studio Esame orale da almeno 40 minuti
Specialista privacy	Prova scritta da 35 domande a risposta multipla e 2 casi studio Esame orale da almeno 30 minuti
Valutatore privacy	Prova scritta da 35 domande a risposta multipla e 2 casi studio Esame orale da almeno 30 minuti

A chi serve davvero una certificazione

Al momento la risposta potrebbe essere "**TUTTI**" per avere una guida univoca all'applicazione dei requisiti del Regolamento e non quella definita dal consulente di turno.

A tendere la risposta potrebbe essere:

- **PMI, soprattutto "P"**
- **fornitori di servizi che vogliono distinguersi sul mercato**
- **fornitori di prodotti che producono che vogliono distinguersi sul mercato**
- **soggetti che sono stati oggetto di violazione**

Ricordiamo comunque che la certificazione resta su base volontaria e non si sa come sarà valutata dall'autorità di controllo.

Conclusioni

Visto che al momento non esiste alcuno schema valido per gli articoli 42 e 43, è consigliabile:

- Utilizzare gli schemi più maturi, riconosciuti, aggiornati e completi (v. **BS 10012 e norma UNI** per i profili professionali)
- Evitare di seguire strade proprietarie proposte da terze parti e anzi richiedere quanto di cui sopra
- Tenere d'occhio costantemente le linee guida del **WP 29** che chiarificano sempre più aspetti e i workshop settoriali
- **Integrare** quanto più possibile la gestione dei dati personali nei sistemi di gestione o negli schemi organizzativi aziendali già esistenti

Grazie per l'attenzione

Fabio GUASCONI

fabio.guasconi@bl4ckswan.com

UNINFO