Dalla data protection alla data governance: il Regolamento UE 679/2016

Certificazioni privacy

Cesare Gallotti

Milano, 30 novembre 2017

Agenda

- Il GDPR e la certificazione privacy;
- Come funziona la certificazione;
- I sistemi di gestione;
- I servizi, prodotti e processi;
- Iniziative italiane;
- Previsoni per il futuro.

Cesare Gallotti

- Lavora dal 1999 nel campo della sicurezza delle informazioni, della qualità e della gestione dei servizi IT.
- Ha condotto numerosi progetti di consulenza per la pubblica amministrazione e per il settore privato. Opera, sia in Italia che all'estero, come Lead Auditor ISO/IEC 27001 e ISO 9001. Ha progettato ed erogato corsi di Quality Assurance e di certificazione Lead Auditor ISO/IEC 27001 e ITIL Foundation.
- Tra gli attestati di studio e i titoli professionali, si segnalano: le certificazioni CEPAS Lead Auditor ISO/IEC 27001, IRCA Lead Auditor 9001:2008, CISA, ITIL Expert e CBCI, la qualifica come Lead Auditor ISO/IEC 20000 e ISO 22301 e il perfezionamento postlaurea in "Computer Forensics e investigazioni digitali".
- E' capodelegazione del WG1 del comitato italiano ISO/IEC SC27 in UNINFO.
- Riferimenti:
  - Web: www.cesaregallotti.it
  - Blog: blog.cesaregallotti.it
  - Twitter: @cesaregallotti

Il GDPR e la certificazione privacy

La certificazione privacy per il GDPR

- Considerando 100: Dovrebbe essere incoraggiata l'istituzione di meccanismi di certificazione e sigilli nonché marchi di protezione dei dati che consentano di valutare rapidamente il livello di protezione dei dati dei prodotti e servizi.
- Art. 42, par. 1: Incoraggiano l'istituzione di meccanismi di certificazione nonché di sigilli e marchi di protezione dei dati allo scopo di dimostrare la conformità al GDPR dei trattamenti.
- Par. 5: La certificazione è rilasciata dagli OdC o dalla DPA competente in base ai criteri approvati dalla DPA o dal Board.
- Art. 43, par. 1: Gli organismi di certificazione sono accreditati da (opzione):
  - la DPA competente;
  - dall'organismo nazionale di accreditamento (regolamento CE n. 765/2008) secondo la EN ISO/IEC 17065:2012 (relativa ai prodotti, processi e servizi) e i requisiti aggiuntivi stabiliti dalla DPA competente.

NOTA: gli articoli del GDPR qui sono stati riassunti.

Dove è citata?

- Art. 24 par. 3: L'adesione ai codici di condotta o al meccanismo di certificazione **può** essere utilizzata come elemento per dimostrare il rispetto degli obblighi del titolare del trattamento.
- Art. 25 par. 3: Il meccanismo di certificazione può essere utilizzato come elemento per dimostrare la conformità ai requisiti di cui ai paragrafi 1 [attuare in modo efficace i principi di protezione dei dati] e 2 [trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento] del presente articolo.
- Art. 28 par. 5: L'adesione da parte del responsabile del trattamento a un codice al meccanismo di certificazione può essere utilizzata come elemento per dimostrare le garanzie sufficienti.
- Art. 32 par. 3: L'adesione a un codice di condotta ol meccanismo di certificazione può essere utilizzata come elemento per dimostrare di garantire un livello di sicurezza adeguato al rischio.

NB: testo adattato.

Ma anche i codici di condotta

- Art. 40: Le associazioni e gli altri organismi rappresentanti le categorie di titolari del trattamento o responsabili del trattamento possono elaborare i codici di condotta.
- Art. 41 (par. 1): il controllo della conformità con un codice di condotta 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.
- Art. 41 (par. 3): L'autorità di controllo competente presenta al comitato il progetto di criteri per l'accreditamento dell'organismo.
- Art 41 (par. 4): un organismo adotta le opportune misure in caso di violazione del codice da parte di un titolare del trattamento o responsabile del trattamento. Esso informa l'autorità di controllo competente di tali misure e dei motivi della loro adozione.

Riflessioni sui codici di condotta

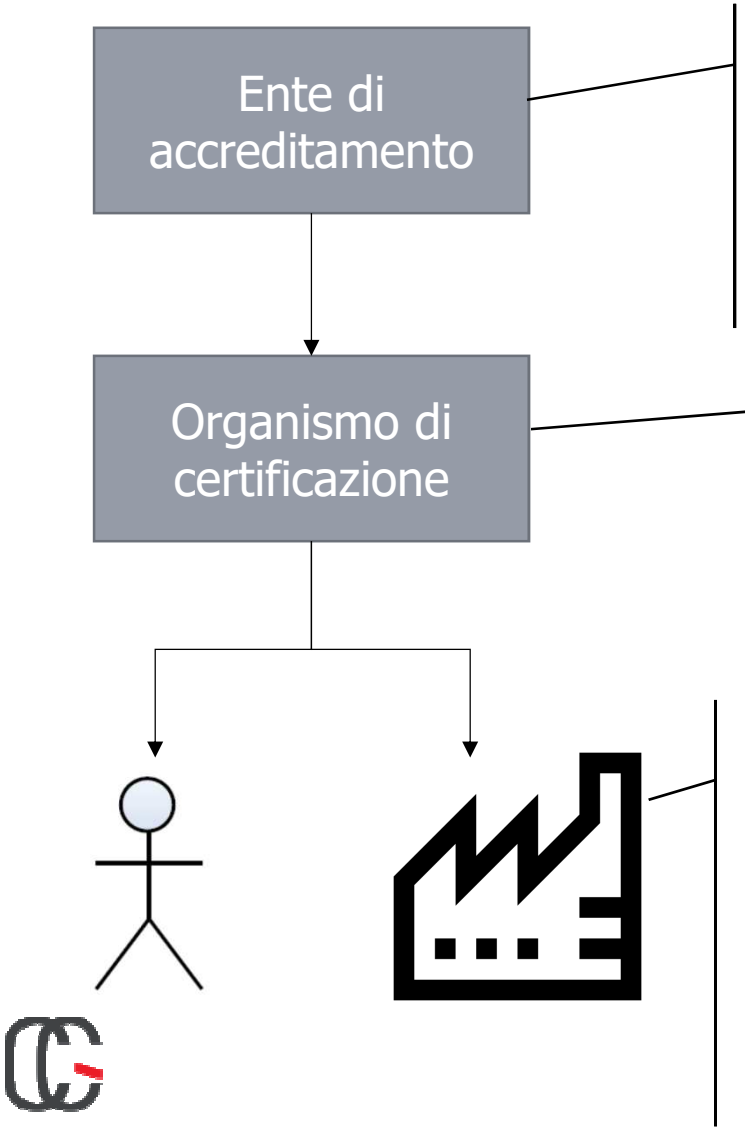
- Sono in corso analisi dei progetti di accreditamento dei soggetti che dovrebbero controllare l'adozione di codici di condotta?
- Conviene, ad un'organizzazione, che l'organismo di controllo informi il Garante per la privacy in caso di non conformità?

Le certificazioni delle persone?

- La posizione più comune è che gli articoli del GDPR relativi alla certificazione non includono le persone.
- In Spagna è stato pubblicato a luglio 2017 uno schema relativo al profilo del DPO.
- In Italia da tempo si sta lavorando (in attesa di prossima pubblicazione) di una norma "Profili professionali relativi al trattamento e alla protezione dei dati personali".

Come funziona la certificazione

Come funziona la certificazione (regolamentata)



- Gli EdA si riconoscono mutualmente (MLA).
- Essi lavorano secondo standard definiti (ISO/IEC 17011).
- Recepiscono anche altre norme.
- Accreditano gli OdC

- Gli OdC lavorano secondo standard definiti (ISO/IEC 17021, 17065, ecc.).
- Certificano organizzazioni e persone secondo "specifiche".

- Persone e organizzazioni soddisfano "specifiche" (es. ISO 9001, UNI 11506, ecc.)
- Le specifiche possono essere pubblicate da chiunque.

Gli attori

- Gli enti di normazione (quelli ufficiali sono regolamentati dal Regolamento europeo 1025/2012) emettono norme;
  - possono essere enti nazionali (UNI e UNINFO, BSI, DIN, eccetera);
  - possono essere enti internazionali (CEN, ISO, IEC);
  - possono essere enti privati (tutti possono scrivere norme!);
- Gli organismi di accreditamento sorvegliano le attività di certificazione;
  - accreditano (e verificano) gli organismi di certificazione secondo norme specifiche;
  - si riconoscono mutualmente;
  - in Europa rispondono al Regolamento europeo 765/2008.
- Gli organismi di certificazione;
  - certificano le organizzazioni o i prodotti, processi e servizi;
  - selezionano gli auditor;
- Le organizzazioni e le persone... si vorrebbero certificare;
  - la certificazione deve avvenire rispetto a norme specifiche.

Gli organismi di certificazione

- Vanno stabilite regole per gli OdC. Per esempio in merito a:
  - modalità di conduzione degli audit;
  - verifiche sulla conduzione degli audit;
  - mantenimento dei certificati (sorveglianza, verifiche in occasione di modifiche);
  - gestione dei reclami;
  - trasparenza e imparzialità;
  - competenze del personale.

Regolamenti

- Gli Enti di accreditamento (soprattutto in Italia!) pubblicano requisiti ulteriori a quelli delle norme ISO per gli OdC.
- Gli Organismi di certificazione devono pubblicare un regolamento relativo alle attività di certificazione dei prodotti, processi e servizi.
- Il regolamento dettaglia alcuni processi generali (p.e. gestione dei reclami dei clienti).
- Il regolamento degli OdC dettaglia come sono svolti gli audit:
  - numero e tipo di verifiche di certificazione, sorveglianza e ri-certificazione;
  - modalità di condivisione del rapporto;
  - tipo di rilievi (classificazione delle non conformità) e loro gestione (p.e. a fronte di non conformità gravi è necessario un audit straordinario entro poche settimane).

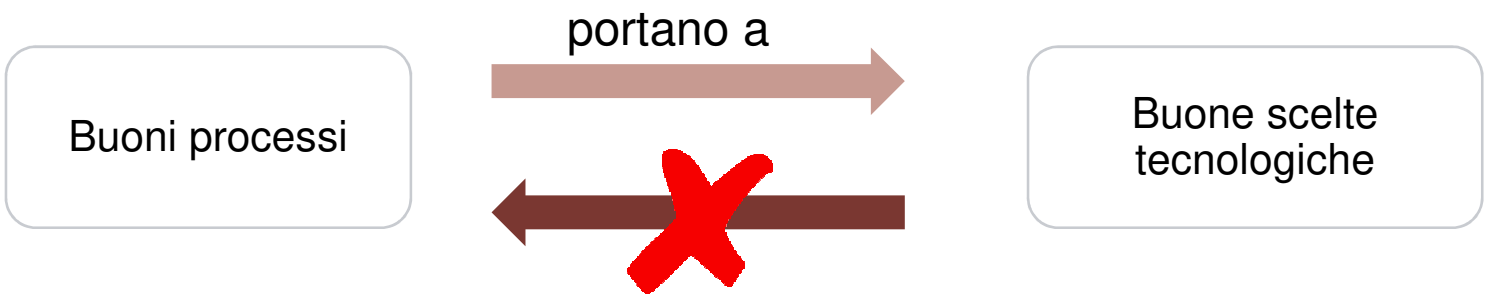
Come funziona la certificazione (parte 2)

- Nessuno vieta di prevedere un "sistema di certificazione alternativo":
  - ente di accreditamento senza accordi con altri enti;
  - ente di accreditamento, in Europa, non rispondente al Regolamento CE n. 765/2008 (ossia in competizione con l'ente nazionale);
  - OdC non accreditato;
  - OdC che eroga alcuni servizi non accreditati;
  - specifiche scritte da enti non "pubblici" o non riconosciuti.
- In alcuni casi, le attività non accreditate hanno come obiettivo di promuovere un sistema "normato" (in altre parole, fungono da prototipi).
- In altri casi, le attività non accreditate hanno come finalità la creazione di un mercato "parallelo" (pertanto non apprezzato da chi promuove il mercato "normato").

I sistemi di gestione

Sistema di gestione per la sicurezza delle informazioni

La sicurezza si basa sulla buona gestione



Processi per: scegliere, attuare, mantenere.

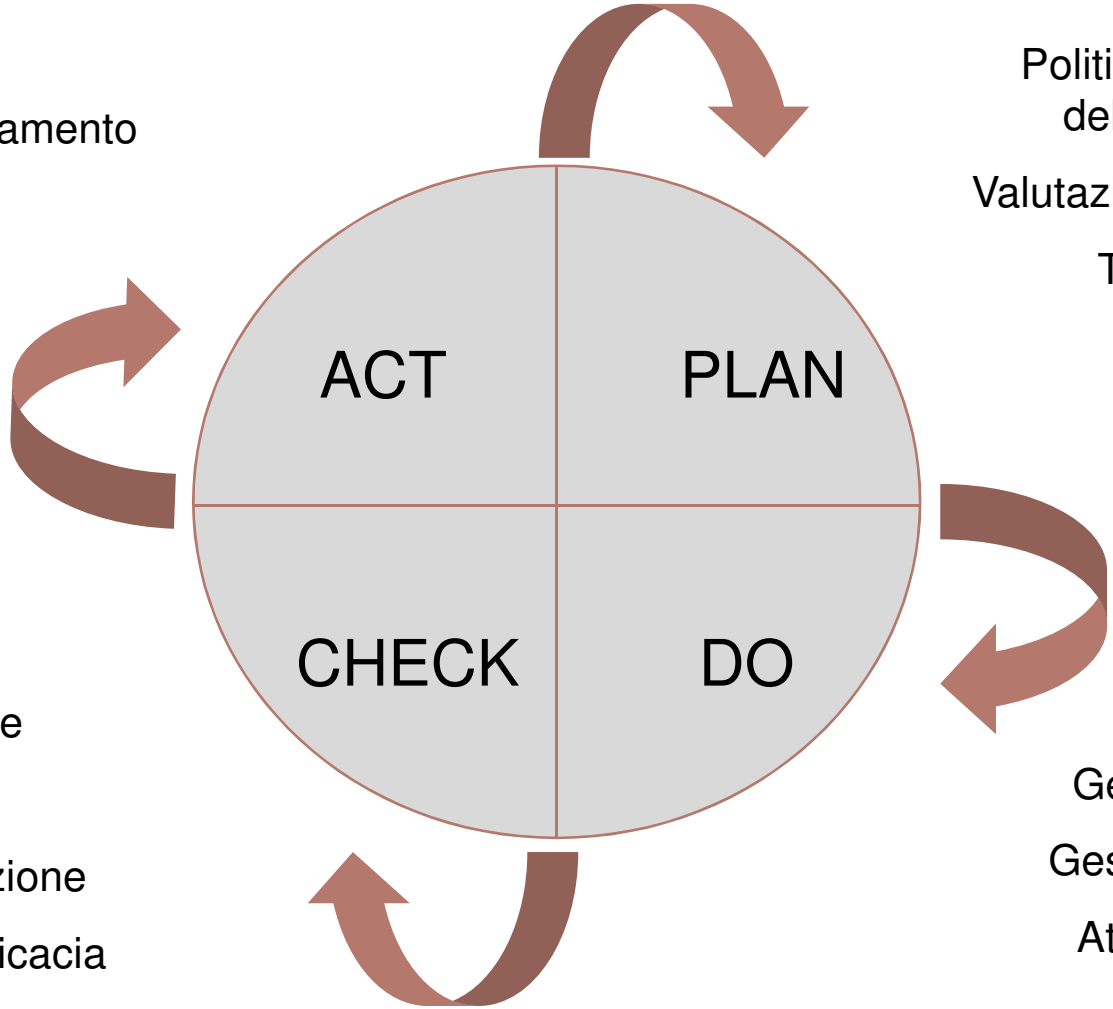
Ciclo PDCA e requisiti di sistema

Leadership

Azioni correttive

Azioni di miglioramento

Aggiornamenti



Politica di sicurezza delle informazioni

Valutazione del rischio

Trattamento del rischio

Verifiche tecniche

Audit interni

Riesame di direzione

Valutazioni di efficacia

Gestire le risorse

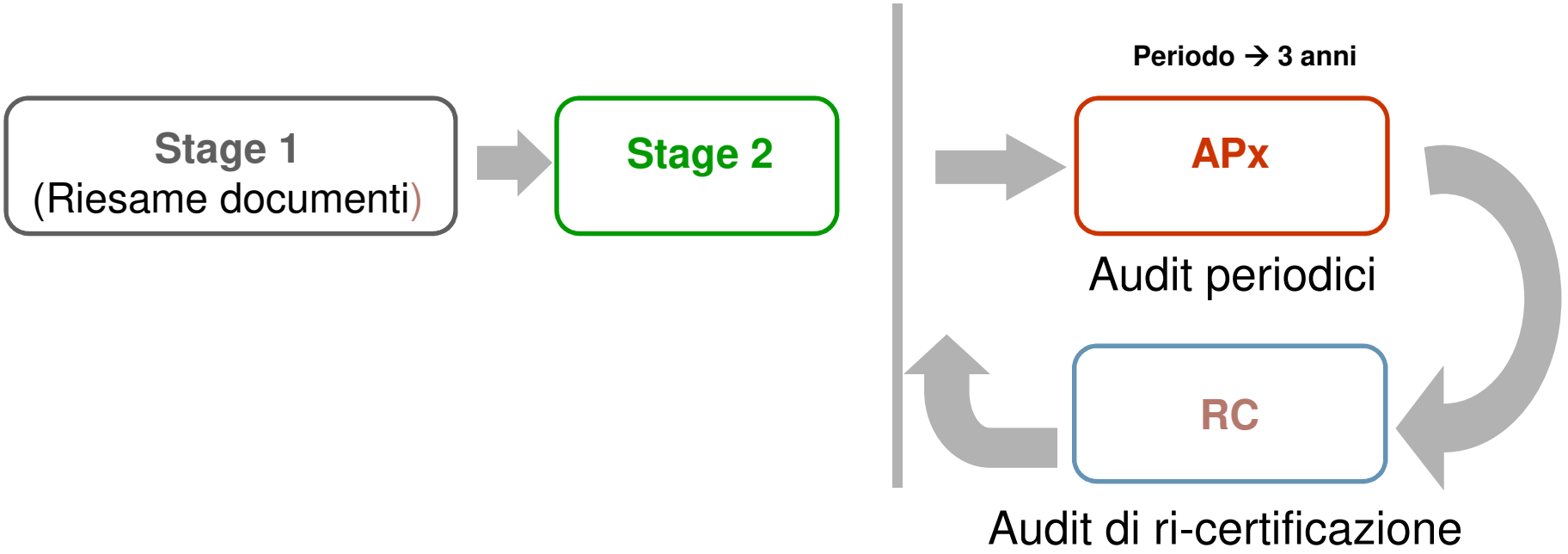
Gestire documenti

Attuare i controlli

Norme note

- Sistemi di gestione noti e diffusi:
  - ISO 9001:2015 per la qualità;
  - ISO/IEC 27001:2013 per la sicurezza delle informazioni.
- Sistemi di gestione per la privacy (standard nazionali):
  - BS 10012:2017 (UK);
  - JIS 15001:2006 (JP);
  - ISO/IEC 29151 (estensione della ISO/IEC 27001 solo per i titolari!);
  - ISO/IEC 27018 (estensione della ISO/IEC 27001 solo per i fornitori di cloud pubblici);
  - ISO/IEC 27552 (di sistema di gestione, estensione della ISO/IEC 27001, e disponibile, forse, da fine 2019).
- Le certificazioni dei sistemi di gestione sono governate dalla ISO/IEC 17021.
- Ma il GDPR cita la ISO/IEC 17065...

Processo di audit di certificazione



- Questo è lo schema tipico di certificazione dei sistemi di gestione.
- Spesso è replicato anche per i prodotti.

Prodotti, servizi e processi

Definizioni

- **Prodotto**: Risultato di un processo; servizi (per esempio, trasporto), software (per esempio, un programma per computer, il contenuto di un vocabolario), hardware (per esempio, la parte meccanica di un motore), materiali da processo continuo (per esempio, un lubrificante).
- **Processo**: insieme di attività correlate o interagenti che trasformano elementi in ingresso in elementi in uscita; esempi sono i processi di tratamento termico, di fabbricazione, di produzione di cibo, di crescita di un impianto.
- **Servizio**: risultato di almeno un'attività necessariamente effettuata all'interfaccia tra il fornitore e il cliente, che è generalmente intangibile; esempi sono: riparazione di un'automobile, elaborazione della dichiarazione dei redditi, erogazione di formazione, messa a disposizione di una camera d'albergo.

Cos’è un trattamento?

- Un trattamento è un:
  - prodotto;
  - processo;
  - servizio?
- Dal considerando 100, si deduce che è un servizio.

Esempi di certificazione di servizio

- Centri di contatto multicanale (norme EN 15838:2010 e UNI 11200:2010)
  - Regolamento Accredia RT-22;
  - la EN 15838 include il ciclo PDCA (strategia, attività operative, riesami periodici, gestione del miglioramento);
- Erogazione di corsi di formazione;
- Vigilanza (norma UNI 10891);
- Centri di monitoraggio e ricezione allarmi (EN 50518 e UNI 11068);
- Fornitori di servizi eIDAS;
  - i requisiti consigliano l'adozione della ISO/IEC 27001;
- Fornitori di servizi di conservazione "a norma" (richiesta la certificazione ISO/IEC 27001);
- Fornitori di servizi SPID (richiesta la certificazione ISO/IEC 27001).

Esempi di certificazione di prodotto

- Attualmente "lo" schema di certificazione della sicurezza dei prodotti informatici è costituito dalla ISO/IEC 15408 (Common Criteria);
  - richiede l'attuazione di processi molto simili (e forse più rigorosi) di quelli richiesti dai sistemi di gestione per la qualità.
- Gli schemi di certificazione di prodotto sono tanti, tra cui:
  - Regolamento Reg. CE 303/2008 (apparecchiature con gas fluorurati);
  - Direttiva PED (per i recipienti in pressione);
  - Direttiva MED (dispositivi medici).
- In molti casi è richiesto un sistema di gestione (per la qualità), anche se non necessariamente certificato.

La certificazione

- Alcuni schemi di certificazione di prodotti, processi o servizi possono comprendere
  - prove iniziali;
  - ispezioni;
  - valutazione dei sistemi di gestione per la qualità, seguite dalla sorveglianza che tiene conto del SGQ e delle prove o ispezioni su campioni prelevati dalla produzione e dal libero mercato.
  - prove iniziali e prove di sorveglianza;
  - solo prove di tipo.

Iniziative italiane

Iniziative italiane

- Il 18 ottobre è stato attivato un gruppo di lavoro per la redazione di una "Prassi di riferimento UNI" dal titolo "Linee guida per la gestione dei dati personali in ambito ICT secondo il Regolamento europeo EU 679/2016 (GDPR)
  - non uno standard di requisiti certificabili;
  - solo per l'ICT (comunque molto importante);
  - comunque un punto di riferimento;
  - prevista la pubblicazione per aprile 2018.
- Di prossima pubblicazione la norma "Profili professionali relativi al trattamento e alla protezione dei dati personali";
  - riguarda DPO, Manager privacy, Specialista privacy, Valutatore privacy;
  - alcuni registri stanno promuovendo schemi di certificazione professionali basati sulle bozze di questa norma.

Previsoni per il futuro

Previsioni (personali)

- Non risultano allo studio delle DPA degli schemi condivisi per i servizi.
- C'è interesse sulla ISO/IEC 27552, ma sarà forse pubblicata solo a fine 2019;
  - si potrebbe trovare una via per cui una norma relativa ai sistemi di gestione possa essere trattata come relativa a servizi;
  - è comunque necessario non prevedere la certificazione come relativa al solo trattamento, ma con impatti su tutta l'organizzazione del titolare o del *processor*.
- Sicuramente alcuni enti promuovono schemi "proprietari" non promossi da alcuna DPA (non secondo criteri approvati da alcuna DPA);
  - vedere anche il comunicato GPD e Accredia del 19 luglio 2017: *in Italia non è ancora stato stabilito dal Legislatore nazionale a chi spetti il ruolo di ente di accreditamento ai fini del regolamento, né sono stati definiti i "requisiti aggiuntivi" per l'accreditamento degli organismi di certificazione.*

Previsioni (personali)

- Schema promosso solo da una DPA (con valore reale solo in un Paese);
  - Label CNIL (dal 2011; 12 label Gouvernance e 1 label relativa ai servizi).
- Schemi promossi... da quale DPA?
  - EuroPriSe (dal 2008, meno di 50 "seals" per prodotti, servizi, siti web);
  - ePrivacy Seal (dal 2011, circa 200 "seals" per prodotti).
- Gli schemi per la certificazione di prodotti;
  - solitamente sono molto complessi da realizzare in ambito IT e molto onerosi da certificare;
  - forse alcuni schemi nazionali (o europeo), meno onerosi dei Common Criteria, si imporranno sul mercato europeo generale.
- Troppi faranno pressioni perché uno schema di "certificazione privacy" sia approvato, ma alcune strade sono percorribili già oggi:
  - audit condotti da persone competenti (non necessariamente di OdC);
  - pubblicizzare le misure di sicurezza adottate.

FINE

Diverse indicazioni sono state raccolte dal Webinar

“Aggiornamento sulle certificazioni collegate al GDPR"

di Fabio Guasconi (Bl4ckSwan S.r.l.)

messo a disposizione da gli Osservatori Digital Innovation del Politecnico di Milano e il Clusit (Associazione Italiana per la Sicurezza Informatica).

Gli errori sono di Cesare Gallotti