CERTIFICAZIONE GDPR, UN'ALTRA CERTIFICAZIONE

Ogni persona ha diritto alla protezione dei dati personali che la riguardano e compito del Regolamento (UE) 2016/679 è la protezione delle persone fisiche. La **certificazione** rappresenta un **efficace istituto** che permette agli interessati di valutare rapidamente il livello di protezione dei dati relativi a prodotti e servizi. **La certificazione ai sensi del GDPR ha regole precise e non coincidenti con gli standard ISMS.**

di Riccardo Giannetti (scheme manager Inveo – presidente Osservatorio679)

ABSTRACT

Il GDPR istituisce un quadro di conformità aggiornato per la protezione dei dati in Europa, basato sul principio di responsabilizzazione e sulla tutela dei diritti fondamentali. Questo nuovo quadro è incentrato su una serie di misure utili ad agevolare la conformità alle disposizioni del regolamento generale sulla protezione dei dati, tra cui le prescrizioni obbligatorie in circostanze specifiche (nomina DPO, Valutazione d'Impatto, ecc) e misure volontarie come i codici di condotta e i meccanismi di certificazione[1].

Ancora prima dell'attuazione del GDPR, il WP29 aveva rilevato come la certificazione potesse ricoprire un ruolo importante nel quadro di responsabilizzazione del titolare[2].

Affinché la certificazione possa fornire prove affidabili della conformità, in termini di protezione dei dati, è opportuno considerare le chiare norme che introducano prescrizioni sulle tipologie e sulle modalità di attuazione delle certificazioni coperte dal Regolamento (UE) 2016/679 e fugare ogni pericolosa confusione su vie di certificazione alternative.

L'articolo 42 del GDPR fornisce la base giuridica per lo sviluppo di tali norme.

I meccanismi di certificazione, per loro stessa natura, possono incrementare la trasparenza non solo per gli interessati ma anche nel quadro delle relazioni tra imprese, ad esempio tra titolare e responsabile. L'istituzione di meccanismi di certificazione, così come indicata dal Regolamento (UE) 2016/679 ("GDPR"), può migliorare la trasparenza e il rispetto del regolamento e consentire agli interessati di valutare il livello di protezione dei dati relativi a **prodotti** e **Servizi**[3]

La certificazione pertanto, quale atto volontario, ha il fine ultimo complessivo di infondere fiducia, a tutte le parti interessate, che un **prodotto** soddisfi i requisiti specificati. Il valore della certificazione quindi è il grado di fiducia e di credito stabilito da un imparziale e competente dimostrazione del soddisfacimento di requisiti specificati, effettuata da una terza parte.

Per tali ragioni la certificazione sotto GDPR dovrà essere una certificazione che nasce in ambiente specifico, con regole specifiche.

[1] EDPB Linee guida 1/2018
[2] WP29 – 173 Opinion 3/2010
[3] Considerando 100 (UE) 2016/679

COS'E' LA CERTIFICAZIONE:

La certificazione[4] è «*il rilascio da parte di un organismo indipendente di un'assicurazione scritta (un certificato) del fatto che il prodotto, il servizio o il sistema in questione soddisfa requisiti specifici*»; nella norma EN-ISO/IEC 17000:2004 a cui la ISO 17065 fa riferimento, la certificazione è definita come "attestazione di terza parte (…) relativa a prodotti, processi e servizi".

SCOPO DELLA CERTIFICAZIONE NEL GDPR:

L'articolo 42(1) prevede l'istituzione (incoraggiamento) di meccanismi di certificazione per dimostrare la conformità al regolamento dei trattamenti effettuati dai titolari e dai responsabili del trattamento. Il contesto in cui la certificazione può essere utilizzata da parte del titolare e del responsabile è riferita in modo particolare a:

a. Attuazione e dimostrazione delle misure tecniche e organizzative adeguate art.24(1)(2), art. 25 e art. 32 (1) (2)
b. Garanzie sufficienti art. 28(1)(4)(5)[5]

Va detto che la certificazione in sé **non è prova di conformità**, ma rappresenta un elemento utilizzabile per la **dimostrazione della conformità** e per tali motivi è necessario attuarla con le modalità previste dal regolamento, in termini di trasparenza, esperienza e metodo.

Il legislatore europeo con l'utilizzo del **termine meccanismo**, nella sua forma plurale «***meccanismi***» (art. 42.1), ha inteso promuovere un sistema basato su **un'ampia pluralità di schemi**, chiarendo di fatto l'impiego della norma internazionale ISO/IEC 17065:2012 per l'accreditamento.

In un articolo del 16 ottobre 2018[6] l'autore ricordava come, già nel settembre 2014, **l'Autorità Garante UK, ICO**, chiedesse a tutti i soggetti interessati (*ICO privacy seals project Framework criteria – draft consultation v.1.3*) documentazione utile **a produrre schemi di certificazione**, «*incoraggiando*» di fatto quanto richiamato dall'art. 42.1.

Più nel dettaglio, il documento richiamava alcuni "criteri" che, gli eventuali **nuovi schemi** di certificazione avrebbero dovuto soddisfare (*pag. 5*):

i. Essere un **nuovo schema** di certificazione protezione dei dati personali
ii. Dover coprire il **trattamento dei dati personali** in U.K. (*non la privacy*)
iii. Essere rivolto al consumatore e **promuovere la fiducia** dei consumatori e la protezione dei dati dei consumatori attraverso la **certificazione di prodotto**

Attraverso la lettura combinata dei termini «incoraggiare» e «meccanismi» con quanto già richiamato nel 2014 dalla autorità UK circa la necessità di sviluppare nuovi schemi, si arriva alla ovvia deduzione che il GDPR richiama la necessità di **sviluppare schemi nuovi**, **specifici** e **compatibili** con la norma ISO/IEC 17065.

Fra gli obblighi che il regolamento definisce in modo non derogabile, ritroviamo:

- l'accreditamento dei CaBs secondo la ISO/IEC 17065 e i criteri aggiuntivi (Annex 1)

[4] Definizione ISO
[5] Linee guida EDPB 1/2018, §1.2
[6] Gdpr, certificazione e accreditamento: che c'è da sapere | https://www.agendadigitale.eu/sicurezza/privacy/gdpr-certificazione-e-accreditamento-che-ce-da-sapere/

- la pluralità di schemi di certificazioni ai sensi della ISO/IEC 17065
- gli schemi di certificazioni "disegnati" sulle prescrizioni del GDPR

Fra gli obblighi, previsti dal Regolamento (UE) 2016/679 ("GDPR"), per gli Organismi di Certificazione (CaBs) vi è infine quello di produrre accurata ed esauriente documentazione e documentare i risultati, al fine migliorare la trasparenza e consentire la ripetibilità di valutazione.

Le informazioni dovrebbero essere facilmente accessibili e comprensibili riguardo i trattamenti certificati e potremmo, per comodità, riassumerle in[7]:

- Descrizione dell'oggetto (c*ampo di applicazione* §3.10 *§7.3.1 - elenco dei prodotti/processi certificati §7.8 ISO/IEC 17065*)
- Indicazione dei criteri approvati applicati (*schema di certificazione utilizzato*)
- Metodologie di valutazione dei criteri (*valutazione §7.4 §7.6 §7.9 ISO/IEC 17065 step 1 e step 2)*
- Periodo di validità del certificato (*documenti riguardanti la certificazione §7.7 ISO/IEC 17065)*
- Comparabilità dei risultati (*Riesame §7.6 ISO/IEC 17065)*

E' necessario rilevare che, sebbene gli stessi elementi siano mandatori per la ISO/IEC 17065:2012, il Regolamento (UE) 2016/679, che richiama proprio la ISO/IEC 17065:2012 quale norma di accreditamento[8], abbia voluto ribadire e rafforzare in via autonoma[9], la necessità di avere una «*certificazione volontaria e accessibile tramite una procedura trasparente* » (art.42(3)).

La **trasparenza** e la **facilità d'impiego** di uno schema di certificazione (*criteri)* e della relativa documentazione rappresentano pertanto condizione necessaria ed imprescindibile affinché vengano prese in considerazione e rispettate le «*esigenze specifiche delle micro, piccole e medie imprese*» (art.42(1)).

Sarà quindi fondamentale redigere correttamente la "documentazione giustificativa" e riportare puntualmente le modalità con cui i criteri vengono soddisfatti (criteri di audit), illustrare le correzioni e le azioni correttive (gestione dei rilievi), descrivere puntualmente le ragioni del rilascio, rinnovo o ritiro di un certificato (rapporto di verifica, sorveglianza) ed infine le conclusioni, le opinioni e le deduzioni derivanti dai fatti e dai presupposti rilevati durante la certificazione (evidenze dell'audit)[10].

Tra le considerazioni degne di nota, si evidenzia che l'EDPB, nel chiarire gli aspetti relativi alla certificazione, abbia sentito l'obbligo (*a parere di chi scrive in modo assolutamente ridondante*) di specificare ulteriormente i requisiti documentali necessari in merito a forme e modalità con cui i CaBs debbano dettagliare le attività di certificazione:

a. metodi e metodologia di valutazione (§5.3)
b. documentazione della valutazione (§5.4)
c. documentazione dei risultati (§5.5)

Un aspetto interessante e pienamente condivisibile, ribadito dall'EDPB, riguarda le possibili "scorciatoie" o le esagerate analisi di dettaglio relative alla certificazione.

Una riduzione del dettaglio della valutazione che si può venire a determinare per scopi pratici o ancor peggio per contenere i costi, potrebbe tradursi in una minore rilevanza della certificazione in materia di

[7] Linee guida EDPB 1/2018, §67
[8] Regolamento (UE) 2016/679 (art. 43(1)(lett.b))
[9] Linee guida EDPB 4/2018 - Annex 1
[10] Linee guida EDPB 1/2018 §14

protezione dei dati; d'altro canto una eccessiva granularità della valutazione potrebbe comportare costi eccessivi e superare la capacità finanziaria del cliente.

Va detto che, al fine della dimostrazione della conformità, potrebbe non essere sempre indispensabile raggiungere un livello molto dettagliato di analisi dei sistemi informatici utilizzati per mantenere la significatività[11].

Altro elemento da rilevare è la mancanza di esperienza e di capacità tecnica degli auditor in ambito protezione dei dati personali, dovuta al fatto che molti CaBs non hanno mai effettuato certificazioni analoghe.

LA CERTIFICAZIONE IN SCOPO ART. 42:

I meccanismi di certificazione della protezione dei dati, ai sensi dell'art. 42, rappresentano una misura volontaria atta ad agevolare la conformità alle disposizioni del regolamento (UE) 2016/679.

Tale misura, quale strumento di regolamentazione volontaria, consente al titolare di «garantire» e «dimostrare» che il trattamento è effettuato conformemente al GDPR (art. 24(1)(3)) e che il **modello organizzativo** adottato risponda ai requisiti previsti.

L'art. 42(1) richiama alcuni elementi fondamentali, ripresi peraltro dalle linee guida EDPB 1/2018:

- gli stati membri hanno il **solo** compito di «**incoraggiare**» l'istituzione di meccanismi di certificazione
- i meccanismi di certificazione possono incrementare la trasparenza non solo per gli interessati ma anche in un quadro di relazioni fra imprese
- devono essere tenute in considerazione le esigenze delle micro, piccole e medie imprese.

Risulta pertanto evidente come **il legislatore europeo** abbia inteso richiamare l'attenzione su meccanismi di certificazione, ispirati **esclusivamente alle regole indicate nel regolamento (UE) 2016/679** e non già ad altri standard internazionali, che per loro natura hanno carattere di copertura universale.

Da queste considerazioni e da quanto indicato dall'art. 43(1)(lett.b) deriva che gli standard ISO maggiormente noti (ISO 27001, ISO 27002 e ISO 27701, etc.) risultano inquadrabili quali certificazioni «**Aspecifiche**»[12] e pertanto **non utilizzabili per la determinazione diretta della conformità**.

Con il termine «*certificazioni aspecifiche*» la Commissione Europea ha inteso indicare quelle norme volontarie rilasciate da enti di standardizzazione internazionale che, seppur non rientranti nelle condizioni indicate dagli articoli 42 e 43 non inquadrabili cioè come «*meccanismi di certificazione della protezione dei dati, ai sensi dell'art. 42*», determinano la possibilità di presidiare alcune aree definite dal regolamento stesso.

Ricordiamo infatti che queste ultime sono accreditabili esclusivamente ai sensi della ISO /IEC 17021-1 o Sistema di Gestione e pertanto non direttamente applicabili quali elementi di comprova.

I CRITERI DI CERTIFICAZIONE:

Gli articoli 42 e 43 definiscono le prescrizioni fondamentali cui si devono ispirare le procedure di certificazione e i relativi criteri.

[11] EDPB linee guida 1/2018 §63
[12] EC Data protection Certification Mechanism – study on article 42 and 43 final report

I criteri di certificazione dovrebbero essere sviluppati concentrandosi sulla «verificabilità, rilevanza e idoneità» di tali criteri ai fini della dimostrazione della conformità al regolamento e pertanto dovrebbero essere formulati per essere chiari, comprensibili e applicabili nella pratica. Per la definizione dei criteri si deve tener conto di alcuni aspetti fondamentali di conformità quali:

- liceità del trattamento (art.6)
- principi del trattamento (art.5)
- diritti degli interessati (artt. da 12 a 23)
- obbligo di notifica delle violazione dei dati (art. 33)
- obbligo protezione sin dalla progettazione (art. 25)
- valutazione d'impatto (art. 35)
- misure tecniche e organizzative messe in atto (art.32)

Cosa sono i «criteri»?

Per «criteri» o «criteri di certificazione» si intendono i criteri in base ai quali viene effettuata una certificazione (valutazione di conformità)[13].

Nella «*certificazione, ai sensi dell'art. 42*» la definizione dei criteri deve passare dall'esatta conversione dei precetti normativi ai controlli operativi attraverso una «*trasduzione*».

La trasduzione è il **processo di conversione** dei principi e delle norme del regolamento generale sulla protezione dei dati personali, in **controlli** operativi sviluppati all'interno di un meccanismo di certificazione che avrà lo scopo di valutare il livello di dettaglio a cui il Titolare del trattamento ha portato la sua conformità al Regolamento.

Chi sviluppa e rilascia i «criteri»?

Il regolamento (UE) 2016/679 non fornisce indicazioni sui soggetti che debbano rilasciare i criteri di certificazione e questa condizione risulta pienamente compatibile con le indicazioni previste nell'art. 43(1)(lett.b) circa l'accreditamento ai sensi della ISO/IEC 17065:2012.

Il regolamento (UE) 2016/679 indica **il compito** delle autorità Garanti: «…approvare i criteri di certificazione conformemente all'art. 42(5)». Art.58(3)(lett.f) e non **rilasciare i criteri di certificazione**.

Questa indicazione pone le Autorità Garanti nella condizione di **valutatori** dei criteri/schemi di certificazione a loro sottoposti via via dagli Scheme Owner che a vario titolo richiederanno l' «**approvazione**» di uno schema.

Con il rilascio degli Annex 1, EDPB linee guida 4/2018, e Annex 2, EDPB linee guida 1/2018, in forma definitiva, sono stati forniti alle autorità di controllo, gli strumenti interpretativi per valutare rispettivamente sia l'accreditamento da parte degli organismi di certificazione (art. 43) che la validità degli schemi sottoposti alla valutazione (art. 42).

Un primo chiarimento ci viene fornito dalle linee guida EDPB 1/2018 in particolare al §28, «**Ruolo dell'organismo di certificazione»,** vengono indicati quali siano i «*soggetti tenuti a definire criteri di certificazione e a istituire procedure di certificazione*»: l'Organismo di certificazione o lo Scheme Owner.

Ulteriore elemento di chiarezza ci giunge dalle linee guida EDPB 4/2018 dove, al §2, fra i soggetti cui sono rivolte le linee guida, sono previsti anche: «altre parti interessate, quali i soggetti che si candidano a operare da organismi di certificazione o i **proprietari di schemi** di certificazione che definiscano i criteri e procedure di certificazione».

[13] EDPB line guida 4/2018 §2

Per rispondere correttamente alla domanda di chi siano i soggetti titolati a «*rilasciare i criteri*» è necessario analizzare sia la figura del «***Proprietario di schema*** *(Scheme Owner, SO)*» che le funzioni dell'«***ISO***» quale ente di normazione internazionale.

Per fare ciò risulta utile confrontare le tre definizioni ufficiali, rispettivamente dell'EA, della ISO/IEC 17065, del GDPR e dell'ISO :

a. **Proprietario dello schema (Scheme Owner - SO)[14]:** viene definita Scheme Owner l'organizzazione identificabile che ha definito un CAS (schema di valutazione della conformità) e che è responsabile per la progettazione del CAS. Si forniscono di seguito alcuni esempi di SO:

   - Enti di Normazione
   - **CABs** (organismi di certificazione)
   - Organizzazioni che utilizzano i servizi dei CAB
   - Organizzazioni che vendono o acquistano prodotti soggetti alla verifica di conformità
   - Produttori o Associazioni di produttori che hanno stabilito un proprio CAS
   - Gli Enti di Accreditamento Nazionali (**NAB**) non possono essere SO

b. **Proprietario dello schema (Scheme Owner - SO)[15]:** Persona od organizzazione responsabile per l'elaborazione ed il mantenimento di uno specifico schema di certificazione. Il proprietario dello schema può essere lo stesso organismo di certificazione, un'autorità governativa, un'associazione commerciale, un gruppo di organismi di certificazione o altri.

c. **GDPR - Scheme Owner[16]:** Il proprietario di uno schema di certificazione è **un'organizzazione identificabile** che ha stabilito i criteri di certificazione e i requisiti in base ai quali va valutata la conformità. L'accreditamento riguarda l'organismo che effettua le valutazioni della conformità (art.43(4)) sulla base dei requisiti dello schema di certificazione e rilascia i relativi certificati. **Il CaB che effettua la valutazione** potrebbe essere la stessa organizzazione che ha sviluppato lo schema di certificazione (criteri), ma potrebbero sussistere accordi in base ai quali un'organizzazione è proprietaria dello schema e un'altra (o più di una) effettua le valutazioni.

ISO (International Organization for Standardization)[17]:

E' la più importante organizzazione a livello mondiale per la definizione di "**norme tecniche**", ha il suo quartier generale a Ginevra in Svizzera e i suoi membri sono gli organismi nazionali di standardizzazione di 164 paesi del mondo.
Può emettere/rilasciare diverse tipologie di documenti:

- **ISO Standards:**
  regole, linee guida o caratteristiche tecniche per le attività produttive o per i loro risultati, volte a raggiungere il grado ottimale (*best practices*) in un determinato contesto. Può assumere molte forme. Oltre agli standard di prodotto, altri esempi includono: metodi di prova, codici di condotta, standard di orientamento e standard dei sistemi di gestione

- **ISO/TS Technical Specifications:**
  contributi che formalizzano specifiche tecniche per la realizzazione di un prodotto o l'erogazione di un servizio. Requisiti di materiali, prodotti, apparecchiature, opere, servizi, organizzazioni, attività, processi, progetti, sistemi, figure professionali, terminologia, convenzioni, metodologie (in generale o per diverse fasi/aspetti del ciclo di vita di ciascuno di questi elementi)

[14] EA 1-22 § 2.2
[15] ISO/IEC 17065:2012 §3.11
[16] Rif.3 EDPB line guida 4/2018
[17] https://www.iso.org/home.html

- **ISO/TR Technical Reports:**
contributi che contengono informazioni di tipo diverso da quelle presenti nelle due precedenti tipologie di pubblicazioni. Può includere dati ottenuti da un sondaggio, ad esempio, o da un rapporto informativo, o informazioni sullo "stato dell'arte" percepito

- **ISO/PAS Publicly Available Specifications:**
specifica tecnica disponibile pubblicamente orientata a rispondere ad un'esigenza urgente del mercato. Essa può rappresentare il parere degli esperti all'interno di un gruppo di lavoro o il parere in un'organizzazione esterna all'ISO

- **IWA International Workshop Agreements:**
accordo internazionale sviluppato al di fuori del normale sistema di normazione per consentire agli operatori del mercato di operare in un ambiente di Open Workshop guidato

- **ISO Guides:**
linee guida sviluppate per comprendere al meglio le aree principali in cui gli standard aggiungono valore.

CERTIFICAZIONE MEDIANTE STANDARD ISO (ISMS)

La normazione volontaria rilasciata dall'**ISO** ed in particolare i Sistemi di gestione delle informazioni e standard derivati, ha il pregio di permettere a tutti coloro che riconoscono questa organizzazione (*164 nazioni aderenti*) di adottare standard equiparabili e confrontabili.

Questa stessa forza potrebbe, letta nell'ottica del GDPR, divenire una debolezza.

Per rendere uniforme uno standard di certificazione sulla «*protezione dei dati*» in tutte le nazioni aderenti alla ISO, sarebbe necessario ricercare soluzioni di compromesso e, in un contesto basato sulla **protezione dei diritti fondamentali delle persone fisiche,** risulterebbe molto complesso da gestire in realtà in cui i diritti fondamentali sono ancora sottoposti a limitazioni.
Il legislatore europeo basandosi sul principio sancito dalla Carta dei diritti fondamentali dell'Unione Europea [18] e dall'art. 16(1) del TFUE ha stabilito che «*ogni persona ha diritto alla protezione dei dati di carattere personale che li riguardano*» definendo così che il diritto alla protezione dei dati personali, a prescindere dalla nazionalità o dalla residenza, è un diritto e una libertà fondamentale.

Un ulteriore spunto giunge dall'EDPB[19]: «*Tuttavia, mentre le norme di settore spesso si concentrano sulla protezione e sulla sicurezza delle organizzazioni nei confronti di eventuali minacce, il regolamento generale sulla protezione dei dati è incentrato sulla protezione dei diritti fondamentali delle persone fisiche. Nella progettazione dei criteri o nell'approvazione dei criteri o dei meccanismi di certificazione sulla base delle norme di settore si dovrà tener conto di tale differenza di prospettiva*»

Pertanto gli schemi di certificazione sotto GDPR (rappresentando uno strumento di accountability e di comprova della conformità) **avranno tale valenza solo e se seguiranno le regole mandatorie indicate dal GDPR.**

Elementi di conferma di questa tesi, giungono dal meccanismo di riconoscimento delle certificazioni fra gli stati membri previsto dal Regolamento (UE) 2016/679; al contrario del principio M.L.A. EA, IAF, ILAC questo non è automatico e scontato, lo stesso deve passare attraverso la proposta dall'autorità garante dello stato proponente, all'EDPB e solo dopo l'approvazione dello stesso, lo schema approvato potrà essere inserito nel registro europeo ed avere validità in tutto il territorio dell'unione.

[18] Articolo 8(1) Carta dei diritti fondamentali dell'Unione Europea
[19] Linee guida EDPB 1/2018 §70

IL LAVORO DELLA COMMISSIONE EUROPEA

La Commissione Europea, ai sensi dell' art. 43 (8) (9) del GDPR, ha effettuato uno studio comparativo su 117 schemi di certificazioni nel mondo. I risultati dello studio commissionato all'Università di Tilburg[20] sono stati pubblicati in un documento di sintesi che evidenzia, allo stato, due schemi già idonei per valutare la conformità al GDPR (uno italiano e l'altro tedesco).

CONCLUSIONI

Per quanto esposto, risulterebbe fuorviante verso i Titolari e i responsabili del trattamento, stimolare o ancor peggio **incentivare,** l'utilizzo di meccanismi di certificazione basati su norme tecniche che per loro stessa natura sono "**ab origine**" fuori scopo art. 42 (***ISO /IEC 27001 - 27701***).

I meccanismi di certificazione per la sicurezza delle informazioni (***ISMS ISO/IEC 17021-1***) avrebbero invece la possibilità di essere utilizzati come norme tecniche "interoperabili" (standard **aspecifici**) per la messa sotto controllo di processi ben definiti dal GDPR (*art. 32 (1)(lett.b)), art.5(1)(lett.f)*).

Questo sarà un elemento essenziale nel momento in cui si dovranno esibire certificazioni come pre-requisito di conformità, ad esempio per partecipare **a bandi di gare pubblici**, pena l'aumento dei ricorsi.

Per tali ragioni la certificazione sotto GDPR dovrà essere una certificazione che nasce in ambiente specifico, con regole specifiche, un'altra certificazione.

[20] Data protection certification mechanism – study on article 42 and 43 of the regulation (EU) 2016/679 – Final Report and annex