“Prassi di riferimento” e simili come «meccanismi di certificazione della protezione dei dati»

Come noto il Regolamento (UE) 2016/679 (“GDPR”) riconosce ai «meccanismi di certificazione di cui all’articolo 42» (o «meccanismi di certificazione della protezione dei dati») specifiche funzioni all’interno del quadro regolatorio introdotto dalla riforma.
I «meccanismi di certificazione della protezione dei dati» sono un valido strumento di regolamentazione volontaria da cui si fanno discendere importanti effetti di accountability e di affidabilità che non possono essere compromessi da iniziative collaterali che non soddisfano le prescrizioni normative e, quindi, non possono sortire i medesimi effetti dei «meccanismi di certificazione della protezione dei dati». Sul mercato si è assistito ad un fiorire di certificazioni in ambito GDPR che, tuttavia, non potevano considerarsi «meccanismi di certificazione della protezione dei dati» per le ragioni anzidette, creando una pericolosa confusione proprio in danno dei profili di accountability e affidabilità citati in precedenza.
Questa puntata si sofferma sulle distinzioni che intercorrono tra i «meccanismi di certificazione della protezione dei dati» ed il collaterale fenomeno di accordi e prassi che non costituiscono “norme tecniche”.

Sintesi

Fig. 1 - Il ruolo dei meccanismi di certificazione della protezione dei dati in ambito GDPR.

Considerate le numerose e delicate funzioni svolte dai «meccanismi di certificazione della protezione dei dati» - importante strumento di *soft law* - il legislatore ha disciplinato con prescrizioni tassative, l’intero procedimento dall’ideazione, vaglio e accreditamento dei pertinenti schemi di certificazione, sino all’individuazione dei soggetti titolati ed alla conseguente procedura di accreditamento degli organismi di certificazione.
Sistemi di certificazione che indirizzano il tema del GDPR, ma che non rispondono esattamente alle prescrizioni in esso previste - così come altri modelli analoghi ma non

rispondenti alle caratteristiche dettate dal regolamento per tali strumenti - non possono qualificarsi come «meccanismi di certificazione della protezione dei dati» e, di conseguenza, non possono produrre i medesimi effetti che il GDPR ricollega a questi ultimi. Questa conclusione vale anche per prassi o accordi e simili che si vorrebbe far rientrare tra i «meccanismi di certificazione della protezione dei dati», considerata la maggiore semplicità del relativo procedimento di realizzazione.

Funzioni dei «meccanismi di certificazione della protezione dei dati»

Secondo il GDPR, l'adesione a un meccanismo di certificazione «*ai sensi dell'articolo 42*» ha lo «*scopo di dimostrare la conformità al presente regolamento dei trattamenti effettuati dai titolari del trattamento e dai responsabili del trattamento*» e, in particolare:

- «*può essere utilizzat(o) come elemento per dimostrare il rispetto degli obblighi del titolare del trattamento*» (art. 24(3), GDPR)
- «*può essere utilizzato come elemento per dimostrare la conformità ai requisiti*» della protezione dei dati by design e by default (art. 25(3), GDPR)
- «*può essere utilizzat(o) come elemento per dimostrare le garanzie sufficienti*» che i responsabili del trattamento ed i sub-responsabili sono tenuti a prestare (art. 28(5), GDPR)
- «*può essere utilizzat(o) come elemento per dimostrare la conformità ai requisiti*» per l'adozione di un adeguato livello di sicurezza (art. 32(3), GDPR)
- costituisce una garanzia adeguata ai sensi dell'articolo 46 per legittimare il flusso di dati personali verso paesi extra-UE che, viceversa, non forniscono garanzie adeguate (art. 46(2)(f), GDPR)
- rappresenta un elemento da tenere in debito conto da parte dell'autorità di controllo nazionale «*(a)l momento di decidere se infliggere una sanzione amministrativa pecuniaria e di fissare l'ammontare della stessa in ogni singolo caso*» (art. 83(2)(j), GDPR).

Di conseguenza, anche se le norme tecniche nascono come norme volontarie, il «meccanismo di certificazione per la protezione dei dati», essendo regolato dal GDPR, ha natura vincolante riguardo alla procedura di formazione ed ai suoi criteri e requisiti.

Accountability

Principio fondante della riforma è la cosiddetta accountability (art. 5(2), GDPR). La versione italiana del regolamento («*Il titolare del trattamento* ***è competente per il rispetto*** *(...) e in grado di comprovarlo*», enfasi aggiunta) non aiuta a "sdoganare" questo concetto non facilmente traducibile nella nostra lingua: un misto di responsabilizzazione, affidabilità, attendibilità, assicurazione, rendicontabilità. Il parere 3/2010 del WPArt29 del luglio 2010 (wp173) si era già posto il problema terminologico precisando che tramite questo termine, «*(i)n generale, comunque,* ***l'accento è posto sulla dimostrazione di come viene esercitata la responsabilità*** *e sulla sua verificabilità. La responsabilità e l'obbligo di rendere conto sono due facce della stessa medaglia ed entrambe sono elementi essenziali di una buona governance. Solo quando si dimostra che la responsabilità funziona effettivamente nella*

pratica può instaurarsi una fiducia sufficiente.». Il parere wp173 va dritto al punto quando afferma che tale principio contribuisce «*a passare "dalla teoria alla pratica"*» ed aumenta il livello di responsabilità del titolare.

Certificazioni GDPR come strumento di accountability

Quindi, punto centrale dell'accountability è la «*dimostrazione di come viene esercitata la responsabilità*», cioè di come si rispettano prescrizioni e garanzie poste dal regolamento.
Dalle funzioni affidate allo strumento dei «meccanismi di certificazione della protezione dei dati», come sopra rilevato, emerge che le certificazioni GDPR sono «*element(i) per dimostrare*»

- «*il rispetto degli obblighi del titolare*»
- «*la conformità ai requisiti*»
- «*le garanzie sufficienti*».

In breve, i «meccanismi di certificazione della protezione dei dati» contribuiscono a dimostrare il rispetto della norma, cioè che l'organizzazione di riferimento sia effettivamente "*accountable*".

Certificazioni GDPR e valutazione sanzionatoria

Ulteriore funzione svolta dai «meccanismi di certificazione della protezione dei dati» si ha nell'ambito sanzionatorio: «*(a)l momento di decidere se infliggere una sanzione amministrativa pecuniaria e di fissare l'ammontare della stessa in ogni singolo caso* ***si tiene debito conto*** *(...) (del)l'adesione ai meccanismi di certificazione* ***approvati ai sensi dell'articolo 42***» [art. 83(2)(j), GDPR, enfasi aggiunta].
"Tenere in debito conto" è espressione analoga a "tenere nella dovuta considerazione", cioè in ambito sanzionatorio l'autorità di supervisione "deve considerare attentamente" l'influenza dell'eventuale adesione dell'organizzazione a «*meccanismi di certificazione approvati ai sensi dell'articolo 42*» sia per stabilire il livello della sanzione ma financo per decidere se irrogare o meno la sanzione stessa. Vale a dire che tali strumenti, allorquando rispondono ai requisiti del GDPR, hanno valenza di esimente totale o parziale dell'eventuale illecito in materia di protezione dei dati personali; ancorchè soggetta all'apprezzamento dell'autorità, in quanto «*(l)a certificazione ai sensi del presente articolo non riduce la responsabilità del titolare del trattamento o del responsabile del trattamento riguardo alla conformità al presente regolamento e lascia impregiudicati i compiti e i poteri delle autorità di controllo competenti*», [art. 42(4), GDPR] .

Certificazioni GDPR come garanzie adeguate

Diversamente dalle casistiche indicate in precedenza, laddove i «meccanismi di certificazione della protezione dei dati» costituiscono un elemento di valutazione indicativo di un'evidenza di conformità, i medesimi «meccanismi di certificazione della protezione dei dati» «*unitamente all'impegno vincolante ed esigibile da parte del titolare del trattamento o del responsabile del trattamento nel paese terzo ad applicare le garanzie adeguate*», assumono essi stessi il valore giuridico di garanzie adeguate a legittimare il flusso internazionale di dati personali [art. 46(2)(f), GDPR].

In tale circostanza, pertanto, il legislatore sottrae la determinazione del valore giuridico dello strumento, alla valutazione dell'autorità di supervisione o, in ultima analisi, del giudice competente: è lo stesso GDPR a stabilire l'effetto giuridico dei «meccanismi di certificazione della protezione dei dati» in questo contesto.

Incoraggiamento all'istituzione e sanzioni per violazioni

Questa breve ricostruzione denota l'importante funzione che il legislatore del regolamento attribuisce ai meccanismi di certificazione "ai sensi dell'articolo 42" tanto che

- impone agli Stati membri e alla Commissione di incoraggiare «*in particolare a livello di Unione, l'istituzione di meccanismi di certificazione della protezione dei dati*»
- impone alle autorità di controllo nazionali di «*incoraggia(re) l'istituzione di meccanismi di certificazione della protezione dei dati (...) a norma dell'articolo 42, paragrafo 1*» (art. 57(1)(n), GDPR)
- impone al comitato europeo di «*incoraggia(re) (...) l'istituzione di meccanismi di certificazione della protezione dei dati*» ai sensi dell'articolo 42
- sanziona con pena pecuniaria amministrativa «*fino a 10.000.000 EUR, o per le imprese, fino al 2 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore*», la violazione degli «*obblighi dell'organismo di certificazione a norma degli articoli 42 e 43*» [art. 83(4)(b), GDPR].

Condizioni e requisiti dei «meccanismi di certificazione della protezione dei dati»

In considerazione di quanto sopra, il legislatore del regolamento si è premurato di stabilire in dettaglio quali siano condizioni e requisiti dei «meccanismi di certificazione della protezione dei dati» idonei a legittimare le molteplici funzioni ad essi assegnate, come sopra rappresentato.
In breve, solo i meccanismi di certificazione che rispondono alle precise condizioni indicate agli articoli 42 e 43 possono qualificarsi come «*meccanismi di certificazione della protezione dei dati, ai sensi dell'articolo 42*» del GDPR e svolgere le funzioni previste dal regolamento. Eventuali ulteriori iniziative provenienti dall'ambito della normazione tecnica nel contesto data protection potranno comunque essere espletate, non essendovi al riguardo alcun divieto normativo ostativo, ma non potranno essere equiparate ai «*meccanismi di certificazione della protezione dei dati, ai sensi dell'articolo 42*» nè svolgere le funzioni che il GDPR assegna a questi ultimi.

Condizioni dell'articolo 43

Tra le ulteriori condizioni che l'articolo detta per i «meccanismi di certificazione della protezione dei dati», l'articolo 43 rubricato "Organismi di certificazione" prescrive che:

- la certificazione (cioè l'oggetto principale del meccanismo di certificazione) sia rilasciata e rinnovata dagli «*organismi di certificazione in possesso del livello adeguato di competenze riguardo alla protezione dei dati*» (art. 43(1), GDPR)
- gli organismi di certificazione siano accreditati dall'autorità di controllo nazionale o dall'organismo nazionale di accreditamento (il codice privacy italiano si è orientato verso l'accreditamento da parte di Accredia, salvo casi particolari; art. 2-septiesdecies, cod. privacy)
- che allorquando gli organismi di certificazione siano accreditati dall'organismo nazionale di accreditamento ciò avvenga «*conformemente alla norma EN-ISO/IEC 17065/2012 e ai requisiti aggiuntivi stabiliti dall'autorità di controllo competente ai sensi degli articoli 55 o 56*» [art. 43(1)(b), GDPR].

Richiamo alla norma EN-ISO/IEC 17065/2012

Da tale ricostruzione si deduce che il richiamo «*alla norma EN-ISO/IEC 17065/2012*» non si riferisce alla sola procedura di accreditamento dell'organismo di certificazione ma si estende anche (se non soprattutto) allo **schema di certificazione** (per accertarne la validità), su cui si basa la certificazione che l'organismo stesso rilascerà ai titolari del trattamento o ai responsabili che dimostrino il rispetto dei requisiti in esso previsti. Tale rispetto (o conformità) viene appunto attestato nella certificazione «ai sensi dell'articolo 42» rilasciata dall'organismo di certificazione accreditato da Accredia.

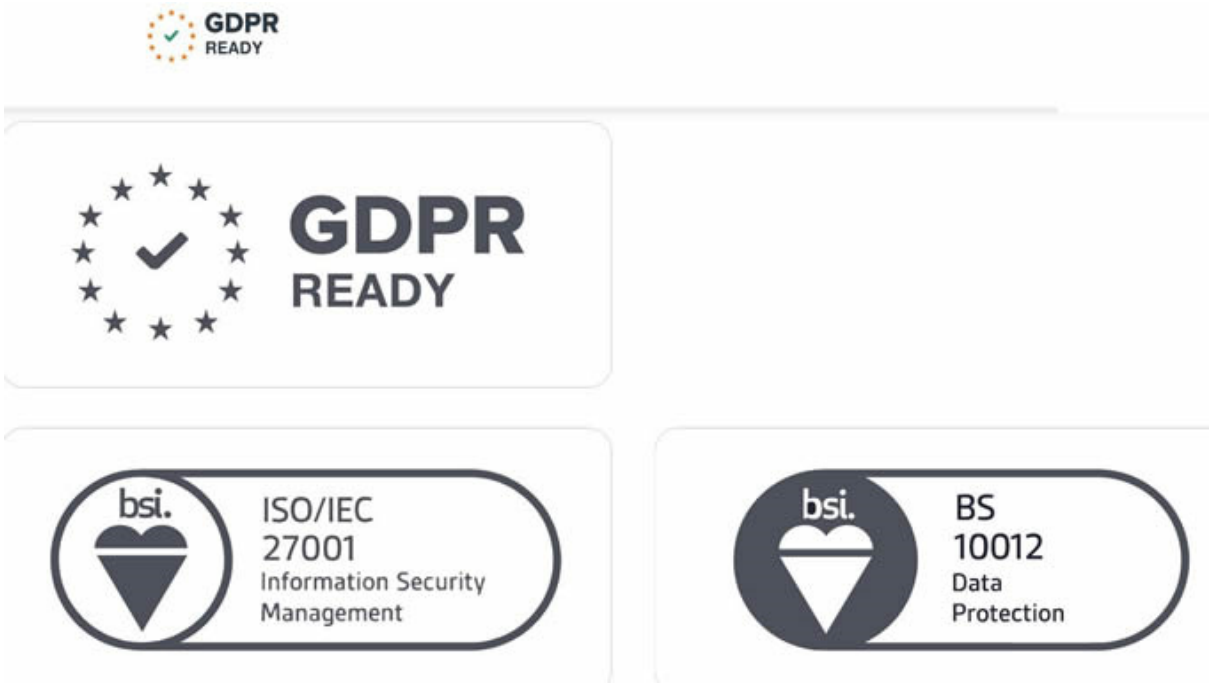

Fig. 2 - I simboli sulla certificazione GDPR già presenti sul mercato ma non il linea col GDPR.

Da tale osservazione ne consegue che eventuali schemi di certificazione che si basassero su normazioni differenti dalla EN-ISO/IEC 17065/2012 - come ISO 27001, ISO 27701 e BS10012 - sarebbero fuori dall'ambito degli articoli 42 e 43 del GDPR e, quindi, non qualificabili come «meccanismi di certificazione della protezione dei dati» da cui far scaturire gli effetti previsti dal GDPR.

Processo del meccanismo di certificazione GDPR

Fig. 3 - Le distinte fasi del «meccanismo di certificazione della protezione dei dati».

Come si nota, quindi, il processo del «meccanismo di certificazione della protezione dei dati» prevede una serie di passaggi (prescrizioni di legge) tutti parimenti essenziali per il raggiungimento dell'obiettivo finale: l'istituzione di un «meccanismo di certificazione della protezione dei dati» ai sensi dell'articolo 42 GDPR, suscettibile di rilasciare una certificazione che sia idonea a svolgere tutte le citate funzioni previste dal GDPR.

Approvazione dei criteri da parte dell'autorità di supervisione

Nella fase iniziale del procedimento per la certificazione GDPR - come indicato nella figura 3 - vi è l'approvazione dei criteri in esso contenuti da parte dell'autorità di supervisione competente, cioè di quella «*del luogo in cui l'organismo di certificazione intende offrire la certificazione e ottiene l'accreditamento*» (linee guida 1/2018, §34).
L'EDPB ha già rilasciato apposite linee guida sia «*relative alla certificazione e all'identificazione di criteri di certificazione*» (1/2018) sia «*relative all'accreditamento degli organismi di certificazione ai sensi dell'articolo 43*» (4/2018).
Peraltro, anche nel caso in cui l'organismo di certificazione intendesse ottenere l'approvazione dei criteri relativi al "sigillo europeo" da parte dell'EDPB (cioè per un meccanismo di certificazione a livello europeo), la domanda per l'approvazione dei criteri da parte del Comitato andrebbe pur sempre presentata per il tramite dell'ASN competente, la quale trasmette il progetto al Comitato, «*se ritiene che i criteri possono essere approvati*» dallo stesso (linee guida 1/2018, § 36).

Criteri di certificazione

Le linee guida 1/2018 sottolineano che i criteri di certificazione sono parte integrante del meccanismo di certificazione e sono suscettibili di approvazione se e quando essi

«*rispecchiano perfettamente il requisito del*» GDPR «*per cui il meccanismo di certificazione consente (...) di dimostrare la conformità al regolamento*». Inoltre, «*(i) criteri di certificazione devono essere approvati dall'autorità di controllo competente prima del processo di accreditamento di un organismo di certificazione o nel corso dello stesso.*».

Tempestività dell'approvazione dei criteri incide su competitività e accountability

Le singole autorità di supervisione nazionali (ASN) sono già nelle condizioni di poter esaminare gli schemi e valutarne l'aderenza dei criteri in essi contenuti rispetto alle indicazioni formulate dall'EDPB.
Risulta chiaro che tale attività, essendo pregiudiziale per l'accreditamento e la successiva certificazione, incide significativamente sui livelli di competitività degli organismi interessati: chi prima otterrà l'approvazione dei criteri del proprio schema dall'ASN competente, avrà un vantaggio competitivo sul mercato rispetto ai concorrenti. Per le implicazioni economiche che ne possono derivare, l'EDPB sottolinea che «*(l)e autorità di controllo sono tenute a trattare tutte le richieste di approvazione dei criteri di certificazione in modo equo e non discriminatorio, in conformità di una procedura pubblica che specifichi le condizioni generali che dovranno essere soddisfatte e che descriva il processo di approvazione.*» (linee guida 1/2018, §33).
Sinora si è a conoscenza della presentazione presso le ASN di taluni schemi per la relativa approvazione dei criteri (es. in Lussemburgo, Germania, Italia) ma non si ha contezza di approvazioni già rilasciate da parte di una ASN.

Meccanismi di certificazione della protezione dei dati e "prassi di riferimento"

Sulla base della ricostruzione normativa e sulle argomentazioni che ne discendono non sembra potersi aderire alla proposta di istituire «meccanismi di certificazione della protezione dei dati», ai sensi dell'articolo 42 GDPR, facendo ricorso alle cosiddette "prassi di riferimento" e similari quale nuova tipologia di documento sia a livello italiano (UNI - Ente nazionale italiano di unificazione) che internazionale (per l'ISO - International Organization for Standardization, le PAS - Publicly Available Specifications; per il CEN - Comitato europeo di normazione, il CWA - CEN Workshop Agreement).

Le PAS dell'ISO

Le PAS sono pubblicate per rispondere a un'esigenza urgente del mercato, che rappresenta alternativamente l'accordo degli esperti all'interno di un gruppo di lavoro o il consenso raggiunto in un'organizzazione esterna all'ISO. Le PAS «*sono pubblicate per l'uso immediato e servono anche come mezzo per ottenere feedback per un'eventuale trasformazione in uno standard internazionale, (esse) hanno una durata massima di sei anni, dopo di che possono essere trasformate in uno standard internazionale o ritirate*» (fonte ISO).

Il CWA del CEN

Un CWA è un accordo sviluppato e approvato in un seminario CEN aperto alla partecipazione diretta di chiunque abbia interesse nello sviluppo dell'accordo, ma non ha lo stato di uno standard europeo e non può confliggere con uno standard europeo. Lo sviluppo di un CWA dura in media tra 10-12 mesi ed esso non può durare più di 6 anni.

Natura delle “prassi di riferimento”

Le “prassi di riferimento” (“PdR”) non sono “norme tecniche” ma «*una forma di documento para-normativo nazionale*» finalizzata a «*consentire in tempi brevi la definizione di accordi specifici, formalizzati sotto forma di disciplinari coordinati dall’intervento strategico dell’UNI*» (fonte: UNI).
«*In sintesi, le prassi di riferimento sono documenti che introducono prescrizioni tecniche o modelli applicativi settoriali di norme tecniche, elaborati sulla base di un rapido (al massimo 8 mesi dall’approvazione della richiesta) processo di condivisione ristretto ai soli autori, verificata l’assenza di norme o progetti di norma allo studio sullo stesso argomento.*». Le PdR durano al massimo due anni.

Caratteristiche comuni di PAS, CWA e PdR

Se ne deduce, pertanto, che PAS, CWA e PdR sono soluzioni adottate dai diversi organismi per rispondere ad esigenze di opportunità e che hanno alcune comuni caratteristiche:

- essi non sono una normazione tecnica ma documenti **para-normativi** che eventualmente possono anticipare una futura normazione tecnica
- **non si basano su alcuna normazione tecnica** di riferimento
- **non possono** innovare o **contrastare norme tecniche** esistenti
- il **processo di condivisione (è) ristretto ai soli autori,** proponenti o partecipanti anzichè a tutti i portatori di interesse, come per le norme tecniche
- il loro **periodo di vigenza è temporalmente limitato.**

Conclusioni

Da tali indicazioni emerge chiaramente che PAS, CWA e PdR non possono essere equiparate ai «meccanismi di certificazione della protezione dei dati», ai sensi dell’articolo 42 GDPR,

- «non essendo documenti normativi» (Fonte: ISO, CEN, UNI) laddove, invece, gli articoli 42 e 43 del regolamento chiaramente indicano la volontà del legislatore a che il «meccanismi di certificazione della protezione dei dati» faccia affidamento su (cioè porti in dote) le garanzie di una tipica norma tecnica che passa attraverso una serie di fasi di analisi e accreditamento
- non essendo basati su alcuna norma tecnica, mentre i «meccanismi di certificazione per la protezione dei dati», accreditati presso l’organismo nazionale di accreditamento, si fondano sulla norma EN-ISO/IEC 17065/2012 [art. 43(1)(b), GDPR].
- avendo un periodo di vigenza temporalmente limitato (massimo 6 anni per PAS, 3+3 anni per CWA, 2 anni per PdR).

In aggiunta, uno dei presupposti che giustificano il ricorso alle “prassi di riferimento” è «l’**assenza di norme o progetti di norma allo studio sullo stesso argomento**», circostanza

questa che appare destituita di fondamento per quanto attiene il tema della protezione dei dati avendo il legislatore fatto ricorso alla citata EN-ISO/IEC 17065/2012 ed essendo stata riconosciuta a livello internazionale (v. studio Università di Tillsburgh) la presenza, allo stato, di due schemi che rispondono al richiamo dell'ISO 17065: uno italiano (ISDP 10003) e l'altro tedesco (EuroPrise).

Rosario Imperiali @Ros_Imperiali