ARTICOLO

Accreditamento e certificazioni alla luce del nuovo Regolamento Privacy. Tra certezze e attese

Filippo Trifiletti – Direttore Generale di Accredia

E' quella attuale una società che ruota e si evolve attorno al valore collettivo del dato, risorsa strategica per lo sviluppo non solo economico ma anche culturale, e per la crescita della conoscenza. Oggi, le nuove tecnologie informatiche e di telecomunicazione hanno un ruolo fondamentale per le attività umane, e la loro pervasività fa emergere priorità e aspetti critici, tra cui la protezione delle informazioni personali, ogni giorno rilevate, trattate e registrate da una moltitudine di soggetti, con strumenti diversi e su molteplici supporti. Spesso l'utente ignora quanti dati personali vengano archiviati, dove, e soprattutto come proteggerli da usi impropri. Questo ha reso impellente, ancor più nel contesto globale dell'economia digitale, l'esigenza di norme comuni, per verificare la capacità dei fornitori dei servizi che gestiscono i dati, di assolvere anche a funzioni di tutela e protezione degli stessi, preservando al contempo i flussi informativi alla base del libero mercato.

A livello europeo, nel maggio 2016, è entrato in vigore il Regolamento UE 679/2016 (GDPR) sulla protezione e sulla libera circolazione dei dati personali, esecutivo dal 25 maggio 2018 in tutti i Paesi dell'Unione europea. Il Regolamento, che in generale introduce regole più chiare in materia di informativa e consenso e limiti al trattamento automatico dei dati personali, nello specifico "incoraggia" l'istituzione di meccanismi di certificazione della protezione dei dati, di sigilli e marchi, con l'obiettivo di attestare la conformità dei trattamenti effettuati dai titolari e dai responsabili del trattamento (art. 42). Vengono indicati sia i soggetti legittimati a rilasciare le certificazioni in modo indipendente, che la differenza tra questi, con eventuale, autonoma, distinta e concorrente facoltà di emettere certificazioni a norma.

Le certificazioni possono quindi essere rilasciate (art. 43) da:

- Organismi di certificazione, che devono essere accreditati dall'Autorità di controllo competente o dall'Ente nazionale di accreditamento designato ai sensi del Regolamento CE 765/2008 – in Italia Accredia – oppure da entrambi. La norma indicata come riferimento per l'accreditamento è la ISO/IEC 17065:2012 che disciplina il rilascio delle certificazioni di prodotto;
- l'Autorità di controllo competente per lo Stato membro – in Italia il Garante per la protezione dei dati personali.

I "criteri" di certificazione, genericamente richiamati dal GDPR, vengono approvati dall'Autorità di controllo oppure dal Comitato europeo per la protezione dei dati istituito dal Regolamento stesso.

Sono gli Stati membri a garantire che l'accreditamento degli organismi di certificazione sia affidato a uno solo o a entrambi i soggetti indicati nel Regolamento. L'Autorità di controllo ha invece la funzione esclusiva di accreditare, in base alla valutazione di requisiti specificati nel Regolamento, i soggetti che verificano la conformità dei titolari o dei responsabili del trattamento che aderiscono a codici di condotta proposti da associazioni o altri organismi delle proprie categorie. L'adesione ai codici di condotta o a un meccanismo di certificazione può essere utilizzata come elemento per dimostrare il rispetto degli obblighi del titolare del trattamento.

Il provvedimento prevede che la Commissione europea potrà adottare atti di esecuzione per stabilire norme tecniche riguardanti i meccanismi di certificazione e i sigilli e marchi di protezione dei dati, nonché le modalità per promuoverli e riconoscerli. Inoltre, accoglie gli indirizzi della UE sul dovere di attenzione speciale verso le micro, piccole e medie imprese, ma non stabilisce quali criteri adottare (prezzo, semplificazione, diversificazione degli schemi di certificazione). Pertanto, dovranno essere formulati indirizzi univoci per assicurare l'uniformità di trattamento dei soggetti che chiedono la certificazione.

La disciplina dell'accreditamento e della certificazione, introdotta dal GDPR, lascia tuttavia altre questioni aperte. Oggetto di analisi sono tuttora gli aspetti legati all'attribuzione delle competenze e responsabilità tra l'Autorità di controllo e l'Ente nazionale di accreditamento, a partire dalle funzioni che può assumere l'Autorità di controllo: normazione, accreditamento, certificazione e vigilanza sull'applicazione dei meccanismi di controllo, se assunte contemporaneamente, configurano delle possibili incompatibilità che meritano attenzione. E' da capire inoltre se la ISO/IEC 17065 debba essere applicabile anche alle Autorità di controllo nel caso in cui queste certifichino.

E rimane da chiarire il fatto che gli schemi di valutazione della conformità potranno avere pesi e campi di applicazione diversi. Ai sensi del Regolamento 679/2016, infatti, gli schemi di accreditamento elaborati sulla base dei criteri approvati dal Comitato europeo diventano schemi validi a livello UE. Dal momento che EA (European co-operation for accreditation), l'infrastruttura europea di accreditamento, non valuta gli schemi regolamentati, spetta al Garante UE della protezione dei dati il ruolo di armonizzare tali schemi tra gli Stati membri. Inoltre, i requisiti di accreditamento aggiuntivi rispetto alla norma ISO/IEC 17065, che in base al GDPR le Autorità di controllo degli Stati membri possono introdurre, non sarebbero coperti dagli Accordi internazionali di mutuo riconoscimento EA MLA e IAF MRA, con potenziali criticità, in particolare, per le aziende multinazionali.

Occorre anche valutare come si potrà conciliare l'attività degli Enti di normazione, sugli stessi temi, con quella della Commissione europea e la diversa possibile valenza degli schemi basati su disciplinari proprietari, norme tecniche o documenti emessi dalla Commissione. Dovrebbe essere infine chiarita anche la valenza attribuita all'adesione ai codici di condotta, in relazione all'ottenimento di una certificazione, e alla loro spendibilità esimente ai fini della responsabilità d'impresa.

Su tali questioni aperte, il Garante per la protezione dei dati personali sta collaborando, a livello europeo, con le Autorità competenti degli altri Stati membri per definire un quadro comune di criteri per l'accreditamento degli organismi e il rilascio delle certificazioni sul mercato.

E' terminata il 30 marzo scorso, e se ne attendono gli esiti, la consultazione pubblica sulle Linee Guida relative all'art. 43 del Regolamento 679, su cui ha lavorato l'*Article 29 Working Party*, gruppo istituito in base all'art. 29 della Direttiva 95/46 e organismo consultivo e indipendente, composto da un rappresentante delle Autorità nazionali di protezione dei dati personali, dal Garante europeo della protezione dei dati e da un rappresentante della Commissione europea.

In Italia, Accredia, in qualità di Ente unico nazionale di accreditamento, supporta il Garante per fornire tutta la sua esperienza in tema di accreditamento degli organismi di certificazione, al fine di garantire la corretta implementazione del Regolamento 679/2016 a livello nazionale. Infatti, il Legislatore non ha ancora stabilito a chi spettino responsabilità e competenze per accreditare gli organismi di certificazione ai sensi del Regolamento. In questo particolare contesto, Accredia e il Garante hanno dunque chiarito[1] che, fino a decisione del Legislatore, le certificazioni di persone, e quelle rilasciate in materia di privacy o data protection, possono senz'altro rappresentare una garanzia e un atto di diligenza verso le parti interessate dell'adozione volontaria di un sistema di analisi e controllo dei principi e delle norme di riferimento, ma non possono definirsi "conformi agli artt. 42 e 43 del Regolamento 679/2016. Questo proprio perché devono ancora essere determinati i "requisiti aggiuntivi" ai fini dell'accreditamento degli organismi di certificazione e i criteri specifici di certificazione.

A oggi Accredia ha accreditato lo schema proprietario conforme alla ISO/IEC 17065, gestito da un organismo che rilascia la certificazione ISDP©10003:2015 dei processi per la tutela delle persone fisiche con riguardo al trattamento dei dati personali – Reg. UE 679/2016. Schema suscettibile di opportuni adeguamenti, quando gli eventuali criteri integrativi di cui agli artt. 42 e 43 del Regolamento verranno rilasciati dal comitato o dall'Autorità nazionale competente.

Una certificazione già attiva in materia di protezione dei dati personali è anche quella conforme alla norma ISO/IEC 27001, che riguarda i sistemi di gestione per la sicurezza delle informazioni, integrata con le linee guida ISO/IEC 27018[2]. Indirizzata ai service providers di public cloud che elaborano dati personali (PII - Personally Identifiable Information) e che agiscano in qualità di Data (PII) Processor, l'implementazione delle linee guida contribuisce a garantire il rispetto dei principi e delle norme privacy, da parte dei providers di public cloud che se ne dotano. Si tratta, tuttavia, di una certificazione di sistema di gestione che viene accreditata ai sensi della norma ISO/IEC 17021-1, e non della ISO/IEC 17065 indicata dal GDPR come riferimento.

È invece in corso di pubblicazione la nuova Prassi di Riferimento UNI "Linee Guida per la gestione dei dati personali in ambito ICT secondo il Regolamento UE 679/2016 GDPR", elaborata dal tavolo di lavoro "Requisiti dei processi di gestione della privacy in ambito digitale" condotto da UNI con la partecipazione di Accredia e degli altri stakeholder. Articolata in un due parti, una di supporto alla definizione e attuazione dei processi di trattamento dei dati personali, e l'altra contenente i requisiti per la conformità, la prassi si rivolge alle organizzazioni che trattano dati con strumenti informatici, con particolare attenzione alle PMI che possono giovarsi di uno strumento di guida standardizzato e coerente con il GDPR.

---

[1] Cfr. Circolare ACCREDIA DC N° 30/2017 "Informativa in merito all'accreditamento prodotto (ISO/IEC 17065) delle certificazioni rilasciate in conformità allo schema ISDP 10003:2015 - Reg. EU 679/2016" in www.accredia.it/documenti.

[2] Cfr. Circolare ACCREDIA DC N° 13/2017 "Informativa in merito all'accreditamento per lo schema di certificazione ISO/IEC 27001:2013 con integrazione della linea guida ISO/IEC 27018:2014" in www.accredia.it/documenti.

La corretta implementazione di azioni efficaci per il trattamento dei dati con modalità IT può diventare uno strumento competitivo per le aziende che vogliono dimostrare la propria conformità, oltre che un metro di giudizio per le Autorità competenti, con il valore aggiunto della certificazione di terza parte indipendente, secondo i requisiti della norma ISO/IEC 17065.

Ma è sul fronte della definizione delle competenze del personale che il Regolamento 679/2016 trova un effettivo elemento complementare nella nuova norma (pubblicata nel novembre scorso) UNI 11697:2017 "Attività professionali non regolamentate – Profili professionali relativi al trattamento e alla protezione dei dati personali – Requisiti di conoscenza, abilità e competenza". Il Regolamento prevede infatti la presenza del Data Protection Officer (DPO) in tutte le aziende pubbliche, in quelle dove il trattamento dei dati presenti rischi specifichi e quelle che trattano "dati sensibili". La competenza del DPO può quindi essere certificata sotto accreditamento, volontariamente, sulla base dei requisiti indicati nella norma UNI 11697, secondo le specifiche indicate da Accredia in apposita circolare[3].

Inoltre, l'Ente ha coinvolto le parti interessate (inclusi UNINFO e il Garante) per definire regole e criteri comuni per tutti gli organismi di certificazione e si auspica che la norma venga promossa a livello europeo (CEN) per le figure professionali del Responsabile della protezione dati, Manager Privacy, Verificatore Privacy e Specialist Privacy.

A fronte di questa esperienza, e dato che l'Italia in materia di tutela della privacy risulta tra i Paesi capofila dell'Unione europea, Accredia continua dunque a fornire al Garante e all'Ente di normazione nazionale tutto il supporto tecnico possibile, garantendo il suo know-how in materia di accreditamento. L'accreditamento è sinonimo di garanzia e affidabilità per istituzioni, imprese e consumatori e le certificazioni accreditate assicurano la conformità di sistemi, processi, prodotti, servizi e persone ai requisiti fissati dalle norme e dagli standard internazionali. In più, grazie agli Accordi di mutuo riconoscimento firmati dagli Enti di accreditamento a livello europeo (EA MLA) e mondiale (IAF MLA), le certificazioni sono riconosciute a livello internazionale. Ci sono quindi tutte le premesse per garantire il cittadino e tutelare il suo diritto fondamentale alla sicurezza e alla protezione delle informazioni personali.

[3] Cfr. Circolare ACCREDIA DC N° 3/2018 "Disposizioni in materia di certificazione e accreditamento per la conformità alla norma UNI 11697:2017 – Profili professionali relativi al trattamento e alla protezione dei dati personali" in www.accredia.it/documenti.

***Accredia** è l'Ente unico nazionale di accreditamento designato dal Governo italiano. Il suo compito è attestare la competenza, l'imparzialità e l'indipendenza di Laboratori e Organismi che verificano la conformità di prodotti, servizi e professionisti agli standard di riferimento, facilitandone la circolazione internazionale e garantendo la protezione di interessi pubblici come salute, sicurezza e ambiente.*

Accredia è un'associazione privata senza scopo di lucro che opera sotto la vigilanza del Ministero dello Sviluppo Economico e svolge un'attività di interesse pubblico, a garanzia delle istituzioni, delle imprese e dei consumatori.

Accredia ha 67 soci che rappresentano tutte le parti interessate alle attività di accreditamento e certificazione, tra cui 9 Ministeri (Sviluppo Economico, Ambiente, Difesa, Infrastrutture e Trasporti, Interno, Istruzione, Lavoro, Politiche Agricole, Salute), 7 Enti pubblici di rilievo nazionale, i 2 Enti di normazione nazionali, UNI e CEI, 13 organizzazioni imprenditoriali e del lavoro, le associazioni degli organismi di certificazione e ispezione e dei laboratori di prova e taratura accreditati, le associazioni dei consulenti e dei consumatori e le imprese fornitrici di servizi di pubblica utilità come Ferrovie dello Stato ed Enel.

L'Ente è membro dei network comunitari e internazionali di accreditamento ed è firmatario dei relativi Accordi di mutuo riconoscimento, in virtù dei quali le prove di laboratorio e le certificazioni degli organismi accreditati da Accredia sono riconosciute e accettate in Europa e nel mondo.