



White paper

Il GDPR,
le certificazioni e la
cybersecurity

**Comitato Scientifico
ASSO DPO
Settore Privato**

White paper

Il GDPR, le certificazioni e la Cybersecurity. Un sinergico scambio di informazioni tra gli attori per il corretto trattamento e la tutela del dato personale.

01

Certificazioni e loro collocazione nella protezione dei dati personali

02

Stato dell'arte delle certificazioni

03

Certificazioni relative alla sicurezza delle informazioni

01. Certificazioni e loro collocazione nella protezione dei dati personali

Un responsabile della protezione dei dati personali dovrebbe conoscere le interrelazioni tra il GDPR, le certificazioni e la cybersecurity, per poter dialogare con gli esperti cybersecurity, con gli organi di certificazione, con i responsabili della funzione IT e, per ultimo ma non certamente ultimo, con il suo titolare o il suo responsabile del trattamento dei dati personali.

Tutto ciò per garantire un sinergico scambio di informazioni tra gli attori che, proprio mantenendo ognuno le proprie specifiche professionalità e responsabilità, vanno tutti nella stessa direzione, quella finalizzata al corretto trattamento e alla tutela del dato personale.

Per iniziare il percorso di questo elaborato, dato il suo oggetto, non si può che cominciare citando il Regolamento relativo alla protezione delle persone fisiche in relazione al trattamento dei dati personali nonché alla libera circolazione di tali dati che tutti ormai conoscono con l'acronimo inglese GDPR (General Data Protection Regulation).

Prima però è opportuno, con l'aiuto del Dizionario Legal Tech curato dai Professori Pierluigi Perri e Giovanni Ziccardi, citare la definizione che della certificazione fa lo stesso Dizionario da pagina 156 e seguenti:

È certificazione quel “processo che prevede l'esecuzione di diverse operazioni di valutazione e accertamento effettuate da soggetti terzi, qualificati e autorizzati, volto ad ottenere il rilascio di un certificato, ovverosia un documento formale che attesti il possesso di determinati requisiti o qualità.”

E ancora “nel contesto privato, invece, la certificazione consiste in un processo di valutazione in merito al possesso di specifiche caratteristiche o requisiti, previsti da una norma tecnica di riferimento (detta anche standard), finalizzato al rilascio di un attestato di conformità (certificato). Gli standard tecnici sono elaborati e approvati da un'organizzazione, nazionale o internazionale, denominata ente di normazione, da non confondere con gli organismi di certificazione che, invece, sono chiamati a verificare il possesso dei requisiti richiesti dalle norme tecniche.

Tra i più importanti enti di normazione si possono citare: ISO (Organizzazione internazionale per la normazione), UNI (Ente nazionale italiano di unificazione) e CEN (Comitato europeo di normazione). Per poter operare gli organismi di certificazione devono essere accreditati presso un ente di accreditamento (in Italia, l'ente unico di accreditamento è ACCREDIA).

A seconda dell'oggetto le certificazioni in ambito privato si distinguono in: i) certificazioni di sistemi di gestione (per esempio: gli standard internazionali "UNI EN ISO 9000" per la qualità, "UNI CEI ISO IEC 27001" sulla sicurezza delle informazioni, ii) certificazioni di prodotti e servizi, e iii) certificazioni di persone (ad esempio, la norma "UNI 11697:2017" per la certificazione di competenze professionali in materia di protezione dei dati personali). (Massimo Farina)".

Gli articoli del Regolamento sono contenuti nella Sezione 5 (intitolata Codici di condotta e certificazioni) del Capo IV (intitolato Titolare del trattamento e Responsabile del trattamento). Osservare come è suddiviso l'articolato di un raggruppamento di norme è necessario e utile per comprendere sia la logica sia il significato che il legislatore, in questo caso europeo, ha rispettivamente avuto e che intende dare alle stesse norme nella loro continuità e nell'intero contesto regolamentare.

Quindi le certificazioni fanno parte del corpo delle norme dedicate al Titolare e Responsabile del trattamento e ciò evidenzia subito che le medesime non sono rivolte alle persone fisiche ma solo agli enti, o meglio ai vari tipi di trattamento di dati personali che gli stessi enti vorranno attuare, che hanno/avranno il ruolo di Titolare o Responsabile del trattamento. Per fare un esempio a tal proposito: le certificazioni non sono previste per i soggetti che, una volta nominati, svolgono il ruolo e le attività demandate al Responsabile della protezione dei dati negli articoli dal 37 al 39.

Proprio a tal fine, si ricorda la sentenza del Tribunale Amministrativo del Friuli-Venezia Giulia, la n.287 del 13 settembre 2018, con la quale ha cassato un bando della Pubblica Amministrazione concernente l'assegnazione dell'incarico di Responsabile della Protezione dei Dati personali, in quanto prevedeva – come requisito – il possesso della certificazione. Certificazione, tra l'altro, nel caso in questione, proprio riguardante la ISO 27001 che sarà illustrata più avanti essendo appartenente quest'ultima al gruppo delle ISO della sicurezza dei sistemi informatici. In particolare, nel bando era stato previsto, come requisito di ammissione alla procedura selettiva, la certificazione Auditor/Lead Auditor ISO/IEC 27001. Il TAR così si esprime: "Sul punto va rilevato che la predetta certificazione non costituisce, come eccepito dal ricorrente, un titolo abilitante ai fini dell'assunzione e dello svolgimento delle funzioni di responsabile della sicurezza dei dati, nell'alveo della disciplina introdotta dal GDPR, dovendosi considerare che: da un lato, la norma ISO 27001 trova prevalente applicazione nell'ambito dell'attività di impresa (basti rilevare che i riferimenti rivolti ad essa, dal legislatore nazionale e dall'ordinamento euro-unitario, attengono essenzialmente ai requisiti degli operatori economici, come ad esempio avviene nel caso dell'art. 93, comma 7, D. Lgs. n. 50 del 2016, in tema di garanzie per la partecipazione alle procedure di affidamento nei settori ordinari); dall'altro lato, la medesima norma, per quanto potenzialmente estensibile all'attività delle pubbliche amministrazioni, fa pur sempre salva l'applicazione delle disposizioni speciali (eurounitarie e nazionali) in materia di tutela dei dati personali e della riservatezza (punto 18 "conformità" della citata norma ISO; cfr. in particolare: 18.1.1 e 18.1.4)".

vuoi consultare il whitepaper completo?

[Iscriviti ad ASSO DPO >](#)

[Area riservata ai soci >](#)