CHIOMENTI

Newsletter

PA Data Protection & Privacy, TMT

DDL Bilancio – Impatti in materia di cybersecurity

14 dicembre 2022

L'attuale articolo 154 del DDL Bilancio prevede l'istituzione di un **Fondo per l'attuazione della Strategia nazionale di cybersicurezza**, finalizzato innanzitutto a finanziare gli investimenti necessari al conseguimento dell'**autonomia tecnologica** in ambito digitale, in modo da garantire la possibilità di detenere un controllo diretto sui dati, attuando, così, **politiche di sovranità delle informazioni.**

Ciò avrà importanti ripercussioni anche sulle aziende, che necessiteranno di un crescente supporto regolamentare in materia di *cybersecurity*.

Infatti, anzitutto, grazie alla creazione di un nuovo organismo per la sicurezza informatica aziendale, saranno realizzati programmi di accelerazione per le PMI e le startup in materia di *cybersecurity*, Inoltre, secondo quanto indicato nella Strategia Nazionale in materia di cybersicurezza, il conseguimento di tale obiettivo passa anche per il **potenziamento delle capacità nazionali di scrutinio e certificazione tecnologica.**

Tali attività sono svolte dal Centro di Valutazione e Certificazione Nazionale (CVCN), istituito in seno all'Agenzia per la Cybersicurezza Nazionale (ACN), che effettua un **articolato e complesso processo di valutazione dei prodotti acquistati** dai soggetti inclusi nel cosiddetto Perimetro di Sicurezza Nazionale Cibernetica (PNSC), ossia un insieme di attori pubblici e privati che erogano servizi essenziali per lo Stato (*e.g.*, energia, trasporti, erogazione del contante).

Tale valutazione ha **importanti ripercussioni** sia sulle aziende incluse nel PNSC, sia sui loro **fornitori** in quanto prevede, tra gli altri, l'obbligo di condizionare, sospensivamente o risolutivamente, i contratti all'esito favorevole dei test di hardware e software che saranno svolti dal CVCN. Tale disposizione normativa ha numerose implicazioni sul piano pratico, quali, ad esempio, la definizione degli adempimenti o degli obblighi di collaborazione imposti in capo a ciascun soggetto, la predisposizione e la negoziazione dei contratti e la strutturazione dei processi interni di *procurement*, anche in considerazione dei tempi estremamente lunghi del processo (che può sospendere l'esecuzione del contratto fino a 6 mesi).

In tale contesto, diventa di crescente importanza per gli attori coinvolti avere un **supporto di advisory.** Infatti, l'incremento delle risorse a disposizione del CVCN (dovuto, tra l'altro, allo stanziamento di alcune somme del DDL Bilancio a favore dell'ACN) fungerà da volano per le attività di tale struttura, che diventeranno maggiormente puntuali e pervasive. Dunque, le aziende necessiteranno di un maggiore supporto nella gestione di tali aspetti.

Il secondo obiettivo del Fondo per l'attuazione della Strategia nazionale di cybersicurezza è l'**innalzamento dei livelli di cybersicurezza dei sistemi informativi nazionali**. Guardando anche al Piano di implementazione della Strategia Nazionale, tale obiettivo sarà conseguito principalmente attraverso:

(i) l'inclusione nel **Perimetro di Sicurezza Nazionale Cibernetica** di ulteriori aziende nazionali. Diventa quindi di fondamentale importanza intercettare tali operatori e proporre loro un supporto legale nella *compliance* normativa;

(ii) lo stanziamento di fondi a favore di infrastrutture nazionali che assicurino l'incremento dei livelli di sicurezza cibernetica delle pubbliche amministrazioni e fornicano adeguate garanzie di autonomia tecnologica del Paese (i.e., il **Polo Strategico Nazionale**, con la conseguente possibilità supportare tale struttura nella *compliance* alla normativa in materia).

Contatti

Gilberto Nava
Partner – Chiomenti
TMT
T. +39.06.46622.719
gilberto.nava@chiomenti.net

Pierluigi Perri
Of Counsel – Chiomenti
Data Protection & Privacy
T. +39.02.721.571
pierluigi.perri@chiomenti.net

Lucrezia Falciai
Associate – Chiomenti
Data Protection & Privacy
T. +39.02.721.571
lucrezia.falciai@chiomenti.net