POSITION PAPER
CLOUD AND AI DEVELOPMENT ACT (CADA)

COM(2026) 502 final & Interinstitutional Procedure Number 2026/0138 (COD)

Per un quadro europeo di sovranità digitale aperto, proporzionato e competitivo

settembre 2026

EXECUTIVE SUMMARY

AmCham Italy condivide l'obiettivo dell'Unione europea (UE) di rafforzare capacità, resilienza e sicurezza nei settori del cloud e dell'intelligenza artificiale. Tuttavia, ci preme rimarcare come, nella formulazione attuale, il CADA rischi di **confondere la "Sovranità Digitale" con la "Nazionalità del Fornitore"**, anziché con il controllo effettivo, verificabile e *auditabile* su dati, servizi e continuità operativa.

Un approccio fondato su criteri di origine, rigida localizzazione e restrizioni verso fornitori di Paesi terzi affidabili potrebbe determinare una riduzione degli spazi di concorrenza, un aumento dei costi per le amministrazioni pubbliche, un generale rallentamento della trasformazione digitale e sostanziali limitazioni all'accesso alle tecnologie più avanzate in materia di cybersecurity e IA.

Per AmCham Italy, il CADA dovrebbe perseguire un modello di **Open Sovereignty**: sovranità come capacità di controllo da parte del cliente/utente finale e come autonomia di scelta, non come chiusura degli spazi di mercato. Le aziende statunitensi che investono in infrastrutture, competenze, ricerca e partnership in Europa contribuiscono in maniera determinante alla capacità digitale europea e devono poter competere sulla base di requisiti tecnici, operativi e di sicurezza proporzionati.

Alla luce di tali considerazioni, si ritiene necessario un riorientamento del testo attuale verso criteri **risk-based, outcome-based e non discriminatori**, coerenti con il Mercato Unico, con gli impegni internazionali sottoscritti dall'UE e con l'esigenza di attrarre investimenti privati in data center e capacità di IA nei diversi Stati membri.

SOVRANITÀ DIGITALE: CONTROLLO VERIFICABILE, NON NAZIONALITÀ

Il punto centrale riguarda l'impostazione dei quattro Union Assurance Levels. Il quadro previsto dal CADA tende a diventare progressivamente più restrittivo non solo rispetto a ciò che i fornitori devono dimostrare, ma anche rispetto a **chi essi devono essere**. Questo approccio rischia di produrre esclusioni basate sull'origine societaria, anziché su evidenze tecniche e operative.

La sovranità dovrebbe essere misurata attraverso strumenti verificabili: cifratura con chiavi gestite dal cliente, *confidential computing*, separazione degli ambienti, controlli di accesso, audit indipendenti, *disaster recovery*, piani di continuità e possibilità di migrazione. Tali misure consentono alle Amministrazioni di mantenere il controllo sui propri dati senza rinunciare alle migliori tecnologie disponibili.

In particolare, i carichi di lavoro pubblici più sensibili, inclusi Difesa, Sicurezza Nazionale e Infrastrutture Critiche, sono proprio quelli che necessitano delle capacità più avanzate in materia di IA, *threat intelligence*, rilevazione delle minacce e risposta agli incidenti. Escludere o limitare i provider globali affidabili può indebolire, anziché rafforzare, l'assetto di sicurezza europeo.

Dati Societari
Via Cesare Cantù, 1
20123 - Milano (MI)
P.IVA 01151000153

Contatti
Phone: +39 02 8690661
Email: amcham@amcham.it
PEC: amcham@pec.it

www.amcham.it

COMPETITIVITÀ, COSTI PUBBLICI E INVESTIMENTI

Un restringimento del numero di fornitori ammissibili comporterebbe minore pressione competitiva e, di conseguenza, maggiori costi per la Pubblica Amministrazione e un minore incentivo ad adottare pratiche e strumenti innovativi. Inoltre, la proposta non appare accompagnata da un'analisi sufficientemente approfondita degli effetti sui bilanci nazionali, sui costi di compliance e sulle catene di fornitura. Si rileva altresì una tensione evidente tra l'obiettivo europeo di attrarre investimenti privati in capacità e data center e un impianto che, di fatto, limita l'accesso alla domanda pubblica proprio per i *global player* maggiormente predisposti e disponibili a investire nelle diverse giurisdizioni dell'UE. Ciò appare tanto più rilevante in questo momento storico, alla luce dell'intenso processo di espansione tecnologica che interessa il contesto socioeconomico europeo. La prevedibilità del quadro regolatorio e l'accesso non discriminatorio al mercato sono condizioni essenziali per mobilitare capitale, competenze e capacità infrastrutturale.

RESILIENZA OPERATIVA E SICUREZZA NAZIONALE

Se la preoccupazione riguarda possibili interruzioni in scenari geopolitici avversi, la risposta più proporzionata non è l'esclusione preventiva dei fornitori, ma la costruzione di un quadro di resilienza operativa. Architetture multi-cloud, piani di uscita, backup, impegni contrattuali di continuità, *service level agreement*, *escrow* e controlli zero-access possono mitigare rischi specifici mantenendo la libertà di scelta dei singoli clienti finali.

La localizzazione dei dati rappresenta solo uno degli elementi che contribuiscono alla sicurezza digitale. La resilienza effettiva deriva dalla combinazione di misure tecnologiche avanzate, capacità di gestione del rischio, continuità operativa e accesso alle migliori competenze disponibili. Per questo motivo, un approccio basato esclusivamente su criteri di localizzazione o di origine del fornitore rischia di non cogliere pienamente i fattori che determinano la sicurezza e l'affidabilità dei servizi cloud.

SUSSIDIARIETÀ, CERTEZZA GIURIDICA E MERCATO UNICO

Il CADA attribuisce alla Commissione europea un ruolo molto incisivo nella definizione della metodologia di *risk assessment* e nella possibile revisione delle valutazioni nazionali. Gli Stati membri sono però i soggetti più vicini alla valutazione della sensibilità dei propri dati, delle funzioni pubbliche e delle esigenze di sicurezza nazionale. Un coordinamento europeo è quindi necessario, con una chiara definizione delle competenze assegnate agli organismi UE e ai singoli governi nazionali.

Al tempo stesso, occorre evitare che l'assenza di definizioni precise generi frammentazione. La nozione di "ordine pubblico" dovrebbe essere circoscritta a casi realmente critici, evitando che funzioni ordinarie della Pubblica Amministrazione siano attratte automaticamente verso livelli più restrittivi. Servono criteri chiari, soglie comuni, metodologia trasparente e pieno coinvolgimento dei co-legislatori.

Dati Societari
Via Cesare Cantù, 1
20123 - Milano (MI)
P.IVA 01151000153

Contatti
Phone: +39 02 8690661
Email: amcham@amcham.it
PEC: amcham@pec.it

www.amcham.it

PAESI TERZI AFFIDABILI E PARTNERSHIP TRANSATLANTICA

Il meccanismo per il riconoscimento dei Paesi terzi associati dovrà essere praticabile, tempestivo e non discriminatorio. Partner democratici, liberali e affidabili, come gli Stati Uniti d'America, sono parte essenziale e integrante dell'ecosistema tecnologico europeo. Un modello in cui i fornitori non-UE sono strutturalmente confinati ai livelli di *assurance* inferiori, salvo decisione discrezionale e non temporalmente vincolata della Commissione, creerà maggiore incertezza e un possibile deterioramento degli Investimenti Diretti Esteri (IDE) nel medio-lungo periodo.

CADA E PUBLIC PROCUREMENT ACT: L'ESIGENZA DI COERENZA SISTEMICA

Un'ulteriore considerazione riguarda la necessità di assicurare piena coerenza tra il quadro del CADA e la proposta di regolamento sugli appalti pubblici e le concessioni, presentata dalla Commissione europea il 9 settembre 2026 (il cosiddetto Public Procurement Act). I due testi, oggi in negoziato parallelo, incidono sul medesimo perimetro della domanda pubblica di servizi cloud e di intelligenza artificiale: il CADA attraverso i quattro Union Assurance Levels, il Public Procurement Act attraverso un quadro orizzontale di preferenza europea e criteri di qualità, sicurezza, resilienza delle catene di fornitura e sovranità.

AmCham Italy ritiene indispensabile evitare che tale sovrapposizione produca un doppio filtro cumulativo sulla stessa procedura di gara, con l'effetto di restringere ulteriormente la platea dei fornitori ammissibili al di là di quanto necessario e proporzionato rispetto alla reale sensibilità dei dati e delle funzioni interessate. In tale prospettiva, si valuta positivamente che la proposta sulla contrattualistica pubblica non contempli un'esclusione automatica e generalizzata dei fornitori di Paesi terzi e preservi espressamente l'accesso degli operatori coperti dall'Accordo sugli appalti pubblici dell'OMC (GPA) e dagli accordi commerciali sottoscritti dall'Unione europea. Si auspica pertanto che lo stesso principio di salvaguardia degli impegni internazionali sia riconosciuto in modo esplicito e simmetrico anche nel CADA, così da garantire certezza giuridica agli operatori, prevedibilità alle Amministrazioni aggiudicatrici e piena coerenza dell'azione normativa dell'Unione. Si raccomanda infine che i due percorsi legislativi siano accompagnati da un chiarimento espresso sui rispettivi ambiti di applicazione e sul rapporto tra le due discipline, evitando duplicazioni di oneri di conformità e assicurando che il complesso dei requisiti resti calibrato su criteri oggettivi, verificabili e proporzionati.

RACCOMANDAZIONI E CONCLUSIONI

Alla luce delle criticità evidenziate, AmCham Italy ritiene quindi opportuno, in riferimento al CADA:

- **Adottare un approccio proporzionato e basato sul rischio**, assicurando che i requisiti di sovranità siano calibrati sulla reale sensibilità dei dati e delle attività interessate, evitando l'applicazione di criteri eccessivamente restrittivi a servizi e funzioni che non presentano particolari profili di criticità.

- **Valorizzare misure di sicurezza e garanzie operative equivalenti**, riconoscendo che la sovranità digitale può essere efficacemente assicurata attraverso controlli tecnici, organizzativi e contrattuali verificabili, in grado di garantire protezione dei dati, continuità del servizio e resilienza operativa.

- **Evitare criteri protezionistici o discriminatori**, sostituendo requisiti basati sull'origine con obblighi dimostrabili di sicurezza, resilienza, interoperabilità e controllo effettivo dei dati.

Dati Societari
Via Cesare Cantù, 1
20123 - Milano (MI)
P.IVA 01151000153

Contatti
Phone: +39 02 8690661
Email: amcham@amcham.it
PEC: amcham@pec.it

www.amcham.it

- **Rendere praticabile il riconoscimento dei partner affidabili**, prevedendo tempi certi, criteri oggettivi e un modello coerente con gli accordi GPA/FTA e con gli impegni commerciali internazionali dell'Unione europea.

- **Limitare l'estensione al settore privato**, sottoponendo ogni eventuale ampliamento ai settori NIS2 a valutazione d'impatto, consultazione degli stakeholder e procedura legislativa ordinaria.

- **Garantire governance equilibrata e certezza giuridica**, definendo la metodologia di *risk assessment* nella normativa primaria e delimitando attentamente i poteri di *override* della Commissione a casi specifici, motivati e proporzionati.

Il CADA può rappresentare un passaggio importante per rafforzare la capacità digitale europea, ma solo se costruito su apertura, proporzionalità e concorrenza. L'Europa ha bisogno di più investimenti, più integrazione, più sicurezza e più accesso alle tecnologie avanzate, non di un quadro che riduca la scelta delle Amministrazioni e indebolisca l'ecosistema dell'innovazione.

In questa prospettiva, **AmCham Italy auspica che il confronto legislativo sul CADA possa condurre a un quadro normativo capace di coniugare efficacemente gli obiettivi di sicurezza, resilienza e autonomia strategica dell'Unione europea** con i principi di apertura, competitività e innovazione che hanno storicamente caratterizzato il Mercato Unico. Ciò richiede un approccio fondato su criteri oggettivi e proporzionati, che valorizzino la capacità effettiva dei fornitori di garantire protezione dei dati, continuità operativa, resilienza delle infrastrutture, trasparenza dei processi e affidabilità dei servizi. In tale contesto, la valutazione dei requisiti di sovranità dovrebbe basarsi su garanzie concrete e verificabili, **evitando meccanismi che possano determinare restrizioni generalizzate** fondate esclusivamente sull'origine societaria o geografica degli operatori. Un'impostazione di questo tipo consentirebbe di rafforzare la sicurezza e la competitività dell'ecosistema digitale europeo, preservando al contempo l'integrità dello spazio economico dell'UE, la capacità di attrarre investimenti internazionali e il valore strategico della collaborazione transatlantica.

Dati Societari
Via Cesare Cantù, 1
20123 - Milano (MI)
P.IVA 01151000153

Contatti
Phone: +39 02 8690661
Email: amcham@amcham.it
PEC: amcham@pec.it

www.amcham.it