ANDERSEN®

novembre 2026

&Compliance Risk Management

Novità normative e pratiche di governance dei dati e di gestione di rischi d'impresa

AI Governance
Fornire e utilizzare sistemi di IA: istruzioni d'uso e responsabilità nella catena di fornitura 2

D.Lgs. 231/2001
Fornitori digitali e rischio 231: perché gli audit della supply chain diventano essenziali 3

Privacy | AI | Cyber
L'importanza della nomina del responsabile del trattamento ai sensi dell'art. 28 GDPR 4

Risk Management
NIS2 e sicurezza nella supply chain: gli obblighi coinvolgono anche chi non è soggetto alla normativa 5



Paola Finetto
Partner
paola.finetto@it.andersen.com



Luca Rigotti
Partner
luca.rigotti@it.andersen.com

Hanno collaborato: **Maria Lillà Montagnani**, **Elisa D'Arrigo**, **Nicolò Bottura** e **Edoardo Lazzaro**

AI Governance

Fornire e utilizzare sistemi di IA: istruzioni d'uso e responsabilità nella catena di fornitura

Quando un'impresa acquista un **sistema di IA** per utilizzarlo nella propria azienda e nei propri processi, chi risponde della sua conformità e dei rischi derivanti dall'utilizzo? L'**AI Act** distingue tra chi sviluppa o fa sviluppare il sistema e lo immette sul mercato con il proprio marchio (*provider*) e chi lo utilizza sotto la propria autorità (*deployer*). Si tratta di ruoli diversi, cui corrispondono obblighi distinti ma strettamente collegati.

Per i **sistemi di IA ad alto rischio**, il **provider** deve fornire istruzioni d'uso che ne illustrino finalità, capacità, limiti, rischi e modalità di supervisione umana. Il **deployer**, a sua volta, deve utilizzare il sistema conformemente alle istruzioni, garantirne la supervisione e monitorarne il funzionamento. Le **istruzioni** diventano così il collegamento tra gli obblighi di chi fornisce il sistema e quelli di chi lo utilizza.

Anche il **contratto di fornitura** assume un ruolo centrale: è opportuno che disciplini la disponibilità della documentazione, gli aggiornamenti, l'assistenza e la cooperazione nella gestione di anomalie e incidenti. Occorre inoltre considerare che, a determinate condizioni, modifiche sostanziali o cambiamenti della finalità d'uso possono comportare l'assunzione degli obblighi del provider da parte del deployer.

La **gestione dei rischi** richiede quindi, da entrambe le parti, chiarezza sulle caratteristiche del sistema, sulle condizioni del suo utilizzo e sulle rispettive **responsabilità**.

D.Lgs. 231/2001

Fornitori digitali e rischio 231: perché gli audit della supply chain diventano essenziali

L'affidamento a fornitori esterni di servizi ICT, infrastrutture cloud e piattaforme digitali rappresenta una prassi sempre più diffusa nelle imprese. **Tale dipendenza, tuttavia, comporta rischi** che possono incidere anche sull'efficacia dei Modelli organizzativi adottati ai sensi del D.Lgs. 231/2001.

Le carenze nei sistemi organizzativi e di sicurezza dei fornitori possono infatti compromettere i presidi aziendali, esponendo l'impresa a vulnerabilità potenzialmente rilevanti rispetto ai **reati informatici** previsti dall'art. 24-bis del Decreto. La semplice esternalizzazione di un'attività, infatti, **non esonera l'impresa** dalla necessità di valutarne le implicazioni in termini di prevenzione dei reati presupposto.

In questo scenario, la valutazione dei rischi 231 non può limitarsi ai processi gestiti internamente, ma deve considerare anche le attività sensibili affidate a soggetti esterni.
Audit periodici, due diligence e monitoraggio continuativo assumono quindi un ruolo essenziale per verificare l'affidabilità dei fornitori, individuare eventuali criticità e accertare l'effettiva applicazione delle misure di controllo.

L'adozione di tali presidi, proporzionata ai rischi delle attività esternalizzate, consente inoltre di documentare le verifiche svolte e gli interventi correttivi adottati, **rafforzando l'effettività del sistema 231**.
La sicurezza della catena di fornitura digitale diventa così parte integrante di una strategia di compliance capace di presidiare i rischi anche oltre i confini aziendali.

Privacy | AI | Cyber

L'importanza della nomina del responsabile del trattamento ai sensi dell'art. 28 GDPR

Ogni impresa affida a soggetti esterni attività che comportano il trattamento di dati personali: elaborazione paghe, servizi cloud, assistenza informatica, CRM, call center. In questi casi il fornitore agisce, di regola, come **responsabile del trattamento** e l'art. 28 GDPR impone al titolare di disciplinare il rapporto con un contratto o altro atto giuridico vincolante.

Non è una formalità. Il titolare può ricorrere solo a responsabili che presentino garanzie sufficienti in merito all'adozione di **misure tecniche e organizzative adeguate**. La nomina va quindi preceduta da una **valutazione della terza parte** (questionari, certificazioni, misure di sicurezza) da documentare e aggiornare nel tempo, in ossequio al principio di **accountability**. L'atto di nomina deve poi prevedere un contenuto minimo: trattamento solo su istruzione documentata del titolare, riservatezza del personale, misure di sicurezza ex art. 32 GDPR, regole sui sub-responsabili, assistenza al titolare (diritti degli interessati, data breach), cancellazione o restituzione dei dati a fine rapporto, **diritto di audit**.

La mancata o inidonea designazione espone l'impresa a **sanzioni** fino a 10 milioni di euro o al 2% del fatturato mondiale annuo (art. 83, par. 4, GDPR). Il Garante ha più volte sanzionato imprese titolari del trattamento per non aver designato fornitori che trattavano dati per loro conto. Senza un contratto chiaro è inoltre difficile controllare il fornitore e ripartire le **responsabilità in caso di incidente**. Il fornitore che determina finalità e mezzi del trattamento è considerato titolare a sua volta (art. 28, par. 10).
Ciò considerato, anche alla luce dell'evoluzione del quadro normativo, diviene fondamentale mappare i fornitori, valutarli e aggiornare gli accordi già in essere.

Risk Management

NIS2 e sicurezza nella supply chain: gli obblighi coinvolgono anche chi non è soggetto alla normativa

Non rientrare nell'ambito di applicazione della **NIS2** non significa restare estranei ai suoi effetti. Il d.lgs. 138/2024 impone ai soggetti essenziali e importanti di presidiare la sicurezza della **catena di approvvigionamento**, considerando anche i rapporti con i **fornitori** diretti di beni e servizi. Un fornitore può diventare, inconsapevolmente, il veicolo di un attacco informatico.

Per questa ragione, anche i soggetti non inseriti nel perimetro NIS2 possono ricevere da loro clienti richieste di adottare misure di sicurezza ICT e cyber, tali da proteggere la infrastruttura informatica e garantirne la **resilienza**, nonché idonee a rilevare tempestivamente **incidenti di sicurezza**.

Non si tratta di una estensione degli obblighi NIS2 a tutti i fornitori. Invero, come chiarito dall'ACN, i requisiti devono essere calibrati sul **rischio** e sulle caratteristiche della fornitura, senza trasferire indistintamente ogni misura prevista per il committente.

Il **contratto** diventa, quindi, uno strumento centrale: occorre definire obblighi verificabili, tempi di comunicazione, controlli e responsabilità, evitando generici impegni di "conformità alla NIS2".

Per le imprese esterne al perimetro normativo NIS2, pertanto, la **sicurezza informatica** non è più soltanto una questione tecnica: può diventare una condizione per ottenere un contratto o mantenere un cliente.