

ottobre 2026

& Compliance Risk Management

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

AI Governance

**Digital Omnibus e AI Act: nuove scadenze per i sistemi
ad alto rischio**

2

D.Lgs. 231/2001

L'intelligenza artificiale nel D.Lgs. 231/2001

3

Privacy | AI | Cyber

**AI Act, Digital Omnibus e GDPR: la ridefinizione delle
basi giuridiche e delle categorie particolari di dati**

4

Risk Management

**Il Risk assessment alla prova dell'IA: nuove attività
sensibili e protocolli per la supervisione umana**

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 Giacomo Obetti**

ottobre 2026

& Compliance & Risk Management

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

AI Governance

Digital Omnibus e AI Act: nuove scadenze per i sistemi ad alto rischio

Nell'ambito del pacchetto di misure volto a semplificare il quadro normativo digitale dell'Unione, il cosiddetto **Digital Omnibus**, le istituzioni europee sono intervenute anche sulla disciplina dell'intelligenza artificiale. Per quanto riguarda l'AI Act, l'intervento non modifica l'impianto del regolamento, ma incide sul calendario di applicazione di alcuni obblighi, in particolare quelli relativi ai **sistemi di IA ad alto rischio**.

Il rinvio più rilevante riguarda quindi i sistemi di cui all'Allegato III dell'AI Act, utilizzati in ambiti quali biometria, infrastrutture critiche, istruzione, lavoro, accesso a servizi essenziali, migrazione e giustizia. Per tali sistemi, gli obblighi si applicheranno dal **2 dicembre 2027**. Se si tratta invece di sistemi ad alto rischio integrati in prodotti regolati, la scadenza è fissata al **2 agosto 2028**.

Il tempo aggiuntivo potrà quindi essere utilizzato dalle imprese per costruire un modello di **AI governance** fondato su una ricognizione concreta degli strumenti già in uso o in fase di adozione. Ciò significa **mappare i sistemi, classificarne il rischio**, individuare ruoli e responsabilità all'interno dell'organizzazione, definire **procedure di approvazione**, adottare regole su dati di input e output e procedere con la **formazione** necessaria. In sostanza, il rinvio delle scadenze permette di affrontare la **compliance** all'AI Act in maniera più ordinata e progressiva, integrandola nei processi di governance, controllo e gestione del rischio già in uso.

ottobre 2026

& Compliance & Risk Management

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

D.Lgs. 231/2001

L'intelligenza artificiale nel D.Lgs. 231/2001

È entrato in vigore il **decreto legislativo n. 160/2026** di adeguamento all'AI Act (Reg. UE 2024/1689), che ha introdotto nel D.Lgs. 231/2001 il nuovo **art. 25-vicies** rubricato «*Delitti commessi mediante l'impiego di sistemi di intelligenza artificiale*».

Il decreto inserisce due reati presupposto nell'articolato sistema della responsabilità amministrativa degli enti. Il primo è l'**art. 437-bis c.p.**, introdotto col medesimo decreto, che punisce l'**omessa adozione di misure tecniche di sicurezza o di sorveglianza umana su sistemi di IA ad alto rischio**, nonché la loro alterazione illecita, a condizione che ne derivi un pericolo concreto per la vita, l'incolumità individuale o pubblica ovvero per la sicurezza dello Stato. Il secondo è l'**art. 612-quater c.p.** che punisce condotte di c.d. deepfake.

Per l'art. 437-bis la sanzione pecuniaria a carico dell'ente va da 600 a 1.000 quote; per il deepfake da 200 a 700 quote. Sono previste misure interdittive, esclusa l'interdizione dall'esercizio dell'attività.

Sotto il profilo 231, sarà quindi necessario verificare, nell'ambito del risk assessment, se e come l'IA, in particolare in sistemi ad alto rischio, venga utilizzata nei processi aziendali. Qualora dall'analisi emerga **un'esposizione concreta al rischio** di commissione dei reati di nuova introduzione, il Modello dovrà individuare specifici **presidi di controllo**, quali criteri e limiti per l'utilizzo dell'IA, definizione dei ruoli e delle responsabilità con riferimento alla generazione e diffusione dei contenuti, meccanismi di controllo e approvazione degli output e adeguati interventi formativi rivolti al personale.

ottobre 2026

& Compliance & Risk Management

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

Privacy | AI | Cyber

AI Act, Digital Omnibus e GDPR: la ridefinizione delle basi giuridiche e delle categorie particolari dei dati

Il 27 luglio 2026 è entrato in vigore il Regolamento (UE) 2026/1744, il cosiddetto "**AI Omnibus**", che modifica l'**AI Act**. Il nuovo testo prevede che i fornitori possano trattare categorie particolari di dati (**cd. dati sensibili**), come i dati relativi alla salute, per rilevare e correggere le distorsioni (**bias**) dei sistemi di IA. Tale facoltà, prima riservata ai fornitori di sistemi di IA ad alto rischio, si estende ora anche ai **fornitori** e agli **utilizzatori** (deployer) di altri sistemi e modelli di IA, nella misura in cui sia garantita l'impossibilità di usare dati sintetici o anonimi, l'adozione di ulteriori misure di sicurezza rafforzata, l'accesso limitato ai dati e la cancellazione una volta corretto il bias. Non si tratta però di un obbligo, né di una deroga al GDPR, che resta pienamente applicabile.

Diverso è il quadro per la parte dell'Omnibus che modifica il **GDPR**, ancora in discussione. La proposta della Commissione Europea chiarisce che il trattamento di dati personali per sviluppare e utilizzare sistemi di IA può fondarsi sul **legittimo interesse** del titolare. Non si tratta però di un via libera automatico: resta necessario il bilanciamento con i diritti degli interessati e le persone devono poter opporsi al trattamento senza condizioni.

Quanto ai dati sensibili, la proposta introduce due nuove eccezioni al divieto dell'art. 9 GDPR. La prima riguarda i **dati sensibili presenti in via residuale nei dataset di addestramento**: sono consentiti se l'impresa adotta misure idonee per evitarne la raccolta e rimuoverli se individuati. La seconda consente l'uso di **dati biometrici per verificare l'identità**, se restano sotto il controllo esclusivo dell'interessato.

In ogni caso, conviene attivarsi per mappare i dati usati nei progetti di IA, verificare la presenza di dati sensibili nei dataset e documentare le basi giuridiche e le misure di sicurezza implementate.

ottobre 2026

& Compliance & Risk Management

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

Risk Management

Il Risk assessment alla prova dell'IA: nuove attività sensibili e protocolli per la supervisione umana

L'IA non deve firmare una decisione per influenzarla. Può scegliere quali candidati mostrare a chi assume, quali guasti segnalare alla produzione o quali clienti sottoporre a verifica. E' uno strumento di supporto mentre la decisione resta umana.

È da qui che parte il risk assessment. Il risk manager mappa gli impieghi dell'IA nei processi aziendali e individua le **attività sensibili**: quelle in cui un errore, un dato distorto o un'informazione omessa può incidere sulle persone, sui risultati economici o sulla **continuità operativa**. Per ciascuna ricostruisce ciò che potrebbe accadere, valuta quanto sia probabile e quale danno produrrebbe. Esamina poi i **controlli esistenti** per capire se il rischio residuo sia accettabile per l'impresa.

Anche la **supervisione umana** deve nascere da questa analisi. Chi approva una previsione deve poter verificare i dati e le ipotesi utilizzate; chi esamina le anomalie selezionate dall'IA deve controllare anche un campione dei casi esclusi. Il protocollo stabilisce chi interviene, in quale momento, con quali informazioni e con quale potere di correggere o fermare il sistema. Le verifiche devono lasciare traccia, così che gli errori rilevati servano ad aggiornare la **valutazione del rischio**.

Il risk manager non aggiunge semplicemente una firma al processo: individua dove l'impresa può perdere il controllo delle proprie decisioni e costruisce le condizioni per continuare a usare l'IA con fiducia.