La conformità dei sistemi di intelligenza artificiale all'AI Act

Appendice 4 al Report Ecomic 3.0



Finanziato dall'Unione europea
NextGenerationEU

MINISTERO DELLA CULTURA

Direzione generale Digitalizzazione e comunicazione

DIGITAL LIBRARY
Istituto centrale per la digitalizzazione del patrimonio culturale

Ecomic
ecosistema
digitale per
la cultura

Appendice 4 del Report Ecomic – ecosistema digitale per la cultura, edizione 3.0, novembre 2026, pubblicato dall'Istituto centrale per la digitalizzazione del patrimonio culturale – Digital Library.

Licenza Creative Commons CC BY-SA 4.0. È consentita la riproduzione, la diffusione e l'adattamento del contenuto del presente documento, a condizione che ne venga citata la fonte e che le eventuali opere derivate siano distribuite con la stessa licenza.
https://creativecommons.org/licenses/by-sa/4.0/deed.it

Il presente documento ha finalità esclusivamente informativa e non costituisce atto amministrativo né prescrittivo.

Ecomic – ecosistema digitale per la cultura

ecomic.cultura.gov.it

Intervento finanziato dall'Unione europea - NextGenerationEU

Nell'ambito del Piano nazionale di ripresa e resilienza, Missione 1 Componente 3

Finanziato dall'Unione europea NextGenerationEU

MINISTERO DELLA CULTURA

Direzione generale Digitalizzazione e comunicazione

DIGITAL LIBRARY
Istituto centrale per la digitalizzazione del patrimonio culturale

Sommario

Introduzione.....4

1. Quadro normativo di riferimento.....6

2. Approccio alla conformità.....8

3. Lo strumento di gestione della conformità 10

4. Lo sviluppo per fasi e le prospettive evolutive.....12

Introduzione

Questa appendice descrive l'approccio con cui Digital Library assicura e documenta la conformità dei sistemi di intelligenza artificiale impiegati nell'ecosistema Ecomic al Regolamento (UE) 2024/1689 (di seguito «AI Act»). Ne illustra i principi, gli strumenti di gestione e le prospettive di sviluppo, a complemento di quanto richiamato nel corpo del Report, definendo come lo strumento di gestione della conformità sia messo a disposizione degli Attori dell'ecosistema.

1. Quadro normativo di riferimento

L'**AI Act**, il Regolamento (UE) 2024/1689, è il regolamento europeo che disciplina l'immissione sul mercato, la messa in servizio e l'uso dei sistemi di intelligenza artificiale secondo un approccio basato sul rischio: distingue le pratiche vietate, i sistemi ad alto rischio, i sistemi soggetti a obblighi di trasparenza e i sistemi a rischio minimo, e gradua gli obblighi in funzione del rischio che il sistema può generare per la salute, la sicurezza e i diritti fondamentali. Sul piano nazionale, la **Legge 23 settembre 2025, n. 132** reca disposizioni e delega al Governo in materia di intelligenza artificiale e individua le autorità nazionali competenti, affidando i relativi compiti ad **AgID** e all'**Agenzia per la Cybersicurezza Nazionale (ACN)**. Gli obblighi applicabili dipendono da due elementi, il ruolo rivestito e la classe di rischio del sistema: il regolamento distingue il **fornitore (provider)**, che sviluppa un sistema e lo immette sul mercato o lo mette in servizio a proprio nome, dall'**utilizzatore (deployer)**, che impiega sotto la propria autorità un sistema realizzato da terzi.

Rispetto ai sistemi impiegati in Ecomic, Digital Library assume un ruolo ibrido: deployer dei modelli di base realizzati da terzi e fornitore (provider) dei sistemi che costruisce e mette in servizio a proprio nome. La qualificazione puntuale del ruolo e la classificazione di rischio dei singoli sistemi, da cui discendono gli obblighi documentali applicabili, sono definite in sede di tavolo compliance. La valutazione del rischio è condotta secondo la metodologia definita da AgID; per i sistemi classificati ad alto rischio la relativa documentazione è trasmessa ad AgID.

2. Approccio alla conformità

L'impostazione adottata parte da un principio: la conformità non è presunta, ma progettata fin dall'inizio e verificata lungo tutto il ciclo di vita del sistema.

Questo principio si traduce anzitutto in scelte architetturali. I sistemi di Ecomic impiegano modelli open source eseguiti su infrastruttura di CINECA: i dati operativi conferiti dagli enti non sono riutilizzati per l'addestramento dei modelli, mentre gli esiti validati dagli operatori possono essere impiegati, in forma controllata, come riferimento per misurarne l'accuratezza. Ne derivano tre effetti rilevanti sul piano della conformità: il contenimento della circolazione dei dati, la riduzione della dipendenza da fornitori proprietari e una minore esposizione a regimi giuridici esterni. Tale orientamento è coerente con l'indirizzo europeo che promuove un'intelligenza artificiale di interesse pubblico, fondata su modelli specialistici di dominio verificabili e governabili dalle istituzioni pubbliche (Raccomandazioni della Community italiana per il governo aperto, 2026).

Sul piano operativo, la conformità poggia su due presìdi:

- **supervisione umana**: gli esiti prodotti dall'IA sono proposti all'operatore per la validazione, identificati come generati dal sistema e non sovrascrivono le informazioni inserite manualmente: l'ente conserva la capacità di verificarli, correggerli o rifiutarli;
- **tracciabilità**: per ciascun sistema è mantenuta una documentazione strutturata che ne segue il ciclo di vita e consente di tracciare le decisioni prese.

3. Lo strumento di gestione della conformità

A sostegno di questo approccio, è stato realizzato un applicativo dedicato alla gestione della documentazione di conformità. Lo strumento guida e facilita la compilazione della documentazione di conformità, dalla classificazione del rischio alla valutazione d'impatto sui diritti fondamentali secondo lo schema di AgID, componendone i relativi allegati. Oltre al supporto alla compilazione, assolve una funzione di governance e monitoraggio: tiene, per ciascun sistema realizzato nell'ecosistema, il fascicolo della valutazione del rischio, ne registra la classificazione secondo i livelli dell'AI Act e ne conserva le revisioni, così che il fascicolo resti allineato alle versioni successive del sistema. L'applicativo è completato nelle sue funzionalità principali, presente negli ambienti di sviluppo, collaudo e produzione, ed è stato oggetto di sperimentazione interna. Concepito come servizio dell'ecosistema, lo strumento sostiene la documentazione dei sistemi di Digital Library e, insieme, è destinato agli Attori che impiegano nella propria offerta i sistemi di intelligenza artificiale del nucleo tecnologico.

All'ingresso l'applicativo presenta il quadro della piattaforma (utenti, statistiche d'uso ed elenco dei progetti), da cui si ha una visione d'insieme dello stato della documentazione dei diversi sistemi e si accede al singolo sistema e alle sue informazioni generali. Il funzionamento è strutturato per ridurre la complessità di compilazione e garantirne la completezza, template per profilo di rischio: per ciascun sistema lo strumento presenta le informazioni richieste in funzione del livello di rischio; alcuni template di approfondimento sono obbligatori, in assenza dei quali la compilazione non è considerata completa e il livello di rischio non si consolida. L'approccio si basa sui seguenti elementi:

- **compilazione per profilo**: le diverse parti sono affidate alle figure competenti di ciascuna organizzazione, tra cui i profili tecnico, legale e della comunicazione, mentre in fase di analisi sono registrati gli stakeholder, ossia i soggetti coinvolti e impattati dal sistema di cui si valuta il rischio;
- **gestione multi-organizzazione**: figure e progetti sono gestiti distintamente per organizzazione, e il riuso degli elementi già compilati da un progetto all'altro consente di alleggerire le valutazioni analoghe.

Completata la compilazione, lo strumento consolida una versione e produce in esportazione un documento nel formato tabellare e documentale richiesto da AgID. La documentazione così prodotta riunisce in un unico fascicolo verificabile gli elementi previsti per il profilo del sistema:

- la classificazione del rischio del sistema;
- la valutazione d'impatto sui diritti fondamentali, per i sistemi impiegati dall'amministrazione;
- gli allegati tecnici corrispondenti al profilo del sistema.

Per i sistemi ad alto rischio si provvede agli adempimenti e alle comunicazioni previsti dalla normativa.

4. Lo sviluppo per fasi e le prospettive evolutive

Lo strumento è stato concepito fin dall'inizio come un sistema completo, destinato a coprire l'intero adempimento documentale previsto dall'AI Act e a essere realizzato per fasi, ciascuna autosufficiente.

La prima fase, oggi completata, mette lo strumento a disposizione dei deployer, le pubbliche amministrazioni che impiegano sistemi di intelligenza artificiale e devono documentarne la conformità e restare aggiornate sui relativi obblighi: è la fase descritta nei paragrafi precedenti, dalla classificazione del rischio alla valutazione d'impatto sui diritti fondamentali secondo lo schema di AgID.

Da questa impostazione discende la dimensione di servizio dello strumento, rivolto agli Attori dell'ecosistema oltre che impiegato internamente da Digital Library. Si articola lungo tre linee:

- **a chi si rivolge**: gli Attori di Ecomic che adottano nella propria offerta i sistemi di intelligenza artificiale messi a disposizione dal nucleo tecnologico assumono il ruolo di deployer e sono tenuti a documentare la conformità del proprio utilizzo;
- **che cosa offre**: il supporto alla compilazione e all'aggiornamento della documentazione di conformità di loro competenza, dalla classificazione del rischio alla valutazione d'impatto sui diritti fondamentali, con l'aggiornamento sugli obblighi quando il quadro normativo cambia;
- **come si colloca**: in continuità con gli altri servizi che l'ecosistema offre agli Attori, grazie all'architettura multi-organizzazione che consente a ciascun ente di gestire distintamente i propri sistemi e la propria documentazione.

La responsabilità della conformità resta in capo a ciascun Attore nel proprio ruolo di deployer; lo strumento ne sostiene la produzione e la tenuta della documentazione.

La seconda fase estende lo strumento al ruolo di fornitore (provider): consente di registrare i dati e la documentazione che competono a chi sviluppa e mette in servizio sistemi di intelligenza artificiale a proprio nome. L'estensione è rilasciata in due momenti, prima i template per la raccolta strutturata delle informazioni e poi il software. Completata questa fase, lo strumento accompagnerà entrambi i ruoli che Ecomic assume nell'ecosistema, deployer e fornitore, lungo un unico percorso documentale.

In questa prospettiva, lo strumento esemplifica un percorso proprio di Ecomic: dalle capacità disponibili oggi l'ecosistema può generare servizi evolutivi che ne estendono il valore. La descrizione dei servizi attuali indica anche le direzioni di sviluppo dell'ecosistema, e la consultazione del mercato è l'occasione per renderle esplicite.

Un orientamento di questo tipo è coerente con il ruolo che le istituzioni culturali possono assumere nella costruzione di un'intelligenza artificiale di interesse pubblico, anche attraverso la condivisione di strumenti comuni.

Ecomic – ecosistema digitale per la cultura è un ambiente collaborativo promosso dal Ministero della cultura per sostenere la trasformazione digitale del settore culturale italiano.

PER MAGGIORI INFORMAZIONI E ADERIRE
ecomic.cultura.gov.it/