FEDERMANAGER
BOLOGNA - FERRARA - RAVENNA

Tecnologia digitale, gestione dei rischi e compliance: come integrare in un progetto di start-up l'applicazione delle norme (iniziamo da GDPR, NIS2 e AI ACT)

Roberto Sammarchi

Il Paradosso della Velocità

Per una startup, la **velocità** è tutto.

La compliance (GDPR, cybersecurity, AI) viene spesso vista come un **freno**.

Ignorare la compliance nei primi 6 mesi non è risparmiare tempo; è accumulare un **"debito tecnico e legale"**.

Questo debito, invisibile all'inizio, esploderà al primo round di finanziamento durante la **due diligence**, diventando una "red flag" insormontabile.

Da Freno ad Acceleratore: La Compliance è un Asset

Il nuovo paradigma è "**Compliance as a Competitive Advantage**".

- **Attrazione Investitori**
  Dimostra maturità gestionale, visione a lungo termine e mitiga i rischi operativi e reputazionali.

- **Abilitazione alle Vendite (B2B)**
  La fiducia è una feature. Il cliente enterprise chiede: "Come gestite i nostri dati? Potete fornire il DPA? Siete conformi a NIS2?"

I Tre Pilastri del "Trust by Design"

GDPR (Privacy)

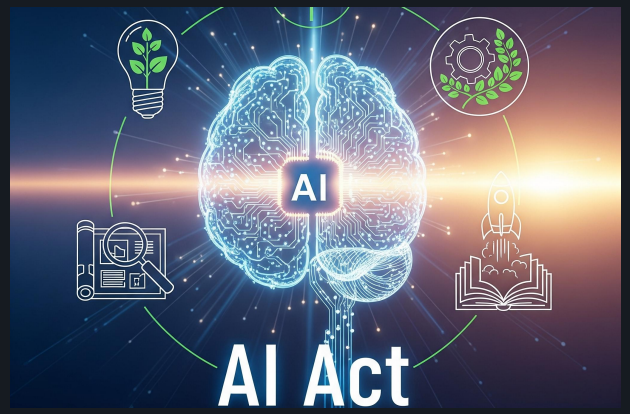
Fiducia nel trattamento dati.

Azione: Minimizzazione.

NIS2 (Security)

Fiducia nella resilienza. Azione:

Gestione supply chain & Notifica 24h.



AI Act (Innovazione)

Fiducia nell'IA. Opportunità:

Regulatory Sandboxes.

AI Act: Triage del Rischio

L'AI Act adotta un approccio basato sul **rischio**. Ecco come una startup può posizionarsi:

INACCETTABILE: App di "social scoring".
→ **Vietato.** Non sviluppare.

ALTO RISCHIO: Piattaforma HR per preselezionare CV.
→ **Piena Conformità** (gestione rischio, supervisione umana).

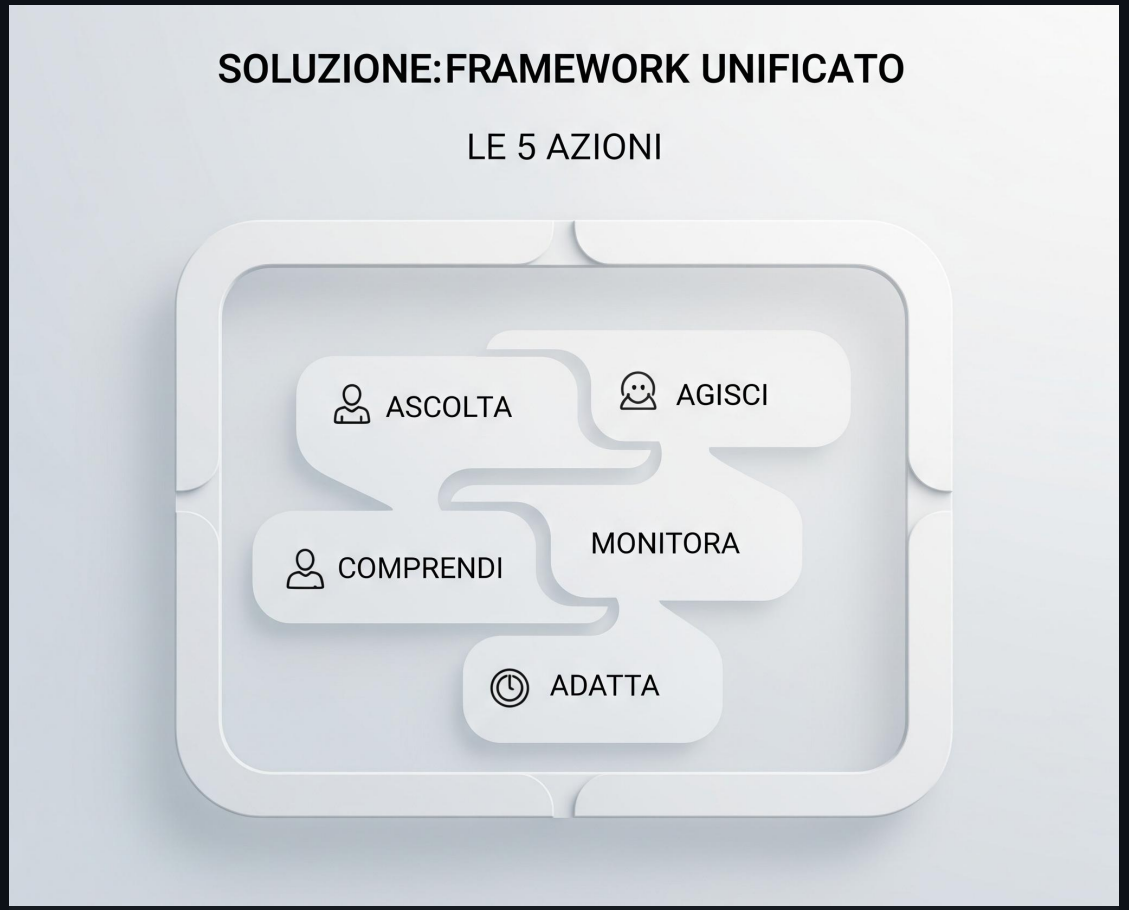
LIMITATO: Chatbot di customer service.
→ **Trasparenza** (l'utente deve sapere che parla con un'IA).

MINIMO: Filtro antispam interno.
→ **Nessuno.** Libero utilizzo.

Soluzione: Framework Unificato (Le 5 Azioni)

Gestire tre norme separate è inefficiente. Serve un unico processo **GRC (Governance, Risk, Compliance)** per gestire gli "obblighi sovrapposti".

1. **1. Valutare e Mappare:** Creare un "Registro Unico" di Dati, Asset IT e Modelli AI.
2. **2. Classificare il Rischio:** Applicare un'unica analisi del rischio.
3. **3. Integrare i Controlli:** Creare un unico set di Misure Tecniche e Organizzative.
4. **4. Documentare (Unificato):** Creare un "Compliance File" unico per gli investitori.
5. **5. Formare il Team:** Creare una "cultura della compliance".



Piano d'Azione: I Primi 6 Mesi

Un piano d'azione pragmatico per una startup appena nata, che copre tutti i regolamenti in modo unificato.

- **Mese 1:** Mappatura e Classificazione (Registro Unico).
- **Mese 2:** Fondamenti Legali e Trasparenza (Privacy/Cookie Policy).
- **Mese 3:** Controlli Tecnici di Base (MFA, crittografia, minimizzazione).
- **Mese 4:** Gestione Fornitori e Contratti (DPA, valutazione sicurezza).
- **Mese 5:** Pianificazione Risposta (Incident Response Plan 24h/72h).
- **Mese 6:** Governance Avanzata (DPIA / Analisi Rischio AI, esplorare Sandboxes).

Conclusione: Dal Debito Legale al Vantaggio Competitivo

- L'Europa sta definendo lo standard globale per un'economia basata sulla **fiducia**.
- Non "aggiungete" la compliance alla fine; **"costruite"** il vostro business *sulle* fondamenta della compliance.
- È il modo più rapido per dimostrare a investitori e clienti che la vostra è un'impresa **seria, resiliente e scalabile**, pronta per il mercato globale.

FEDERMANAGER
BOLOGNA - FERRARA - RAVENNA

Grazie per l’attenzione!