AI WEEK®

THE EUROPEAN #1 AI EVENT

AI WEEK 2026 · STARTUP STAGE

Fiera Rho Milano · 19–20 Maggio 2026

TALK · 20 MINUTI · A DUE VOCI

Agenti AI in azienda: conformi per design.

Tre domande che ogni organizzazione si pone — e tre risposte concrete.

NORMA

Massimo Simbula

Head of Compliance

TECNICA

Davide Carboni

Head of Information Security

TOMATOBLUE

REGTECH · NORMA + TECNICA

Tomato Blue fa RegTech.

Trasformare gli obblighi regolatori — GDPR, AI Act, ISO — in soluzioni operative, con il minimo costo per l'organizzazione.

Oggi, in 20 minuti, vi proponiamo tre domande che ogni azienda con agenti AI si sta facendo. Per ognuna: la risposta della norma, la risposta della tecnologia, e una soluzione concreta che potete vedere all'opera.

IL FORMAT · 3 PUNTATE × 3 SLIDE

?	DOMANDA Entrambi	30 sec
§	NORMA Massimo	2.5 min
⚙	TECNICA Davide	2.5 min

01

CHE COS'È UN AGENTE AI PER IL DIRITTO?

DOMANDA · 01

Un agente AI è un soggetto, un oggetto o un servizio?

L'AI Act classifica i sistemi per rischio ex-ante. Un agente cambia comportamento al volo: low-risk come assistente, high-risk come decisore autonomo. Come lo trattiamo?

NORMA
Massimo Simbula

TEMA 1 · NORMA

Approccio risk-based + GPAI: la norma classifica ex-ante un fenomeno che è in-itinere.

AI ACT · 4 LIVELLI DI RISCHIO

Inaccettabile
Vietati: social scoring, polizia predittiva, scraping massivo, riconoscimento emozioni in lavoro/scuola

Alto rischio
Ammessi se conformi: gestione rischio, governance dati, sorveglianza umana, FRIA, marcatura CE

Rischio limitato
Trasparenza: l'utente deve sapere di interagire con un sistema AI (chatbot, deepfake)

Rischio minimo
Nessun obbligo specifico (filtri spam, sistemi di raccomandazione di base)

GPAI · TRASVERSALE
Modelli general-purpose (Art. 51+): trasparenza, doc. tecnica, AI literacy. Rischio sistemico oltre 10^{25} FLOPs.

DIGITAL OMNIBUS · 19 NOV 2025

Differimento alto rischio: 2 dic 2027 (Annex III) · 2 ago 2028 (Annex I)

Trilogo del 28 apr 2026 chiuso senza accordo. Prossimo: 13 mag. Fino all'adozione, le scadenze originarie restano vincolanti.

IL PROBLEMA APERTO

La categorizzazione statica non regge con entità adattive.

Un agente low-risk come assistente diventa high-risk come decisore autonomo. La piramide non si muove al runtime.

TECNICA
Davide Carboni

TEMA 1 · TECNICA

L'agente è un asset IT certificabile, non un soggetto giuridico nuovo.

ANNEX SL · UNA FAMIGLIA DI STANDARD

ISO 9001
QUALITÀ
Processi, ripetibilità del servizio.

ISO 27001
SICUREZZA INFORMAZIONI
Riservatezza, integrità, disponibilità.

ISO 42001
GESTIONE AI
Risk assessment, lifecycle, oversight.

ISO 27001 · A.5.9 — INVENTORY OF ASSETS

Ogni agente ha un owner, un ciclo di vita, controlli di accesso — come un dipendente digitale.

ISO 42001 · AI MANAGEMENT SYSTEM

Impact assessment del modello, lifecycle, human oversight. Adottabile oggi — senza aspettare il trilogo.

SCHEDA ASSET · AGENTE AI

"Clodia R Olivay" — assistente operativo

OWNER	Davide Carboni · Information Security
MODELLO	GPAI · Anthropic Claude / o1
TOOL PERIMETER	mail · calendar · CRM (read) · billing (read)
HUMAN OVERSIGHT	Approvazione esplicita per write & external send
LIFECYCLE	Onboarding → review trimestrale → offboarding
LOGGING	A.8.15 events · A.8.16 monitoring (≥ 6 mesi)

02

CHI TRATTA I DATI QUANDO DECIDE L'AGENTE?

DOMANDA · 02

Si può fare la DPIA su qualcosa che cambia ogni runtime?

Il GDPR vuole identificare il trattamento ex-ante. L'agente decide al volo quali tool chiamare, tratta dati in modo non deterministico, evolve nel tempo.

NORMA
Massimo Simbula

TEMA 2 · NORMA

AI Act ↔ GDPR: due regimi, un processo. Ma la titolarità diventa mobile.

AREA	AI ACT	GDPR
Valutazioni d'impatto	FRIA · art. 27	DPIA · art. 35
Categorie particolari	Art. 10(5) — bias detection	Art. 9 — divieto + eccezioni
Decisioni automatizzate	Sorveglianza umana · art. 14	Art. 22 ADM
Trasparenza	Art. 13, 50 + watermarking	Art. 13–14 informativa
Registri & log	Art. 12 + 26(6)	Art. 30 trattamenti
Enforcer	AI Office + autorità nazionali	DPA + EDPB

IL NODO APERTO

La titolarità del trattamento diventa mobile.

L'agente decide al volo quali tool chiamare, su quali dati. L'accountability dinamica è territorio grigio nel 2026.

SCHEMA INTEGRATO

AI Act **+ GDPR** **+ Data Act**

Riusare DPIA per costruire FRIA. Riusare i registri art. 30 per i log art. 12. La compliance privacy è un acceleratore — non un onere parallelo.

TECNICA
Davide Carboni

TEMA 2 · TECNICA

La DPIA non si fa sul modello. Si fa sul perimetro dei tool.

DELIBERAZIONE · LLM

Opaca. Non auditabile nel dettaglio.

```
> "Quale tool chiamo per la fattura del cliente X?"
// 32B parametri, decisione probabilistica, non deterministica
```

- Si documenta il modello e i suoi vincoli
- Si definiscono guardrails e prompt di sistema
- Non si pretende auditabilità del singolo passaggio

AZIONE · TOOL-USE

Enumerabile. Loggabile. DPIA-able.

```
tool.invoke("crm.search", { q: clientId })
→ log: agent=clodia, ts=2026-05-19T10:14Z
→ data: 1 record · scope=read · audit: ✓
```

- I tool definiscono il perimetro del trattamento
- ISO 27001 A.8.15 (logging) + A.8.16 (monitoring)
- Ogni invocazione è un event sorgente per la DPIA

!

CAUTIONARY TALE

RAG e data leakage: i permessi ereditati possono esporre dati sensibili. La sicurezza dell'agente è la sicurezza dei suoi tool.

03

VIETARE LO SHADOW AI O SOSTITUIRLO?

DOMANDA · 03

I tuoi dipendenti usano già ChatGPT. Cosa fai?

NDA violati, dati clienti su server senza DPA, perimetro di sicurezza bypassato. Vietare non funziona — ma non vietare nemmeno.

NORMA
Massimo Simbula

TEMA 3 · NORMA

Shadow AI: la legge non dice come risolvere. Dice che il titolare risponde.

COSA STATE GIÀ VIOLANDO

Violazione GDPR
Dati personali su server non coperti da DPA adeguato. Trasferimento extra-UE non documentato.

Violazione NDA
Dati aziendali in modelli third-party senza garanzie di non-training.

Sicurezza compromessa
Perimetro bypassato: nessun log, nessun audit, nessun controllo accessi.

RACCOMANDAZIONE OPERATIVA

Vietare non funziona. Non vietare nemmeno.

Dotarsi di un agente aziendale ufficiale è oggi la mossa di mitigazione più efficace.

COSA FARE OGGI

01 Mappare i sistemi AI già in uso — anche quelli "gratuiti"

02 Classificare il rischio e identificare il ruolo (provider/deployer)

03 Integrare AI Act e GDPR — non duplicarli

TECNICA
Davide Carboni

TEMA 3 · TECNICA + DEMO

L'agente aziendale conforme — elimina il bisogno di Shadow AI.

Boundary definiti
L'agente sa cosa può e non può fare. Policy operativa.

Data residency
Nessun dato personale esce dal perimetro aziendale.

Audit trail completo
Ogni azione loggata. ISO 27001 A.8.15/16.

Compliance by design
ISO 42001 lifecycle + GDPR Art. 25.

TRE TAKE-AWAY

RegTech: trasformare gli obblighi in opportunità operative.

01

L'agente è un asset IT, non un soggetto giuridico nuovo.

Inventarialo in ISO 27001.

02

La DPIA si fa sul perimetro dei tool, non sul modello.

Separa deliberazione da azione.

03

Lo Shadow AI si elimina sostituendolo, non vietandolo.

Un agente conforme è la mitigazione.

GRAZIE. DOMANDE?

Massimo Simbula
Head of Compliance
m.simbula@tomato.blue

Davide Carboni
Head of Information Security
d.carboni@tomato.blue

TOMATOBLUE

WWW.TOMATO.BLUE

SCAN ME