oltrecode

Privacy · Cybersecurity · Trasformazione digitale per la PA

OTTOBRE IN WEBINAR 2026 · DISPENSA

Incontro 4
Intelligenza Artificiale

AI Act, DPIA e FRIA: un metodo per governarla

Data	Venerdì 30 ottobre 2026
Orario	9.00 – 11.00, in diretta
Relatore	Marco La Diega, fondatore di OltreCode

L'intelligenza artificiale è già entrata negli uffici: dal basso, con il dipendente che usa un chatbot, e dall'alto, con il gestionale che aggiunge una funzione di IA con un aggiornamento. In entrambi i casi il Titolare ne risponde. Questa dispensa non vuole spaventare né entusiasmare: offre un metodo.

1 Che cos'è l'intelligenza artificiale

- **È un software** — non è magia e non è un cervello. È un applicativo fatto da persone, con dati scelti e regole decise da persone. Come ogni software, può sbagliare.
- **Come impara** — il modello viene addestrato su enormi quantità di testi e dati. L'addestramento può proseguire anche con i giudizi degli utenti, il pollice su o giù: chi dà un feedback può influenzare le risposte future.
- **Deterministico o probabilistico** — una calcolatrice, alla stessa domanda, dà sempre la stessa risposta. L'IA generativa calcola la risposta più probabile: due domande uguali possono avere risposte diverse.
- **Le allucinazioni** — il modello non sa di non sapere. Può inventare fonti, sentenze e articoli di legge che sembrano veri, e lo fa con sicurezza. Per questo il controllo umano non è facoltativo.

> **L'IA è uno strumento potente, fatto dall'uomo e quindi fallibile:** chi la usa risponde del risultato.

2 I quattro presìdi per governare l'IA

Sono il minimo che ogni ente e ogni azienda dovrebbe avere per non subire l'IA, ma governarla.

1. **Governance: chi se ne occupa.**
   Un responsabile o un gruppo di lavoro che decide quali strumenti si usano, li autorizza e risponde alle domande dei dipendenti. Senza un nome e un ruolo, nessuna regola funziona.
2. **Regolamento d'uso e divieti: cosa si può fare.**
   Una policy scritta, breve e chiara, con gli strumenti autorizzati e quelli vietati. In un chatbot non si inseriscono mai dati personali, dati sanitari, atti riservati, dati di cittadini o clienti.
3. **Mappatura: cosa stiamo usando, anche senza saperlo.**
   Censire gli strumenti di IA in uso, comprese le funzioni attivate in automatico dalle software house con un aggiornamento. Qualcuno deve monitorare e aggiornare la mappa nel tempo.
4. **Controlli: come verifichiamo le regole.**
   Chi controlla, ogni quanto, con quali evidenze. Una regola senza controllo resta sulla carta: è l'accountability dell'Incontro 1.

A tenere insieme i quattro presìdi c'è la formazione: l'AI Act prevede che chi usa sistemi di IA garantisca al proprio personale un livello sufficiente di alfabetizzazione in materia (art. 4).

Lecito o rischioso? Tre esempi

Uso	Attenzione a
Riassumere una delibera	Va bene con strumenti autorizzati e atti già pubblici; il riassunto va sempre riletto e verificato
Scrivere la risposta a un cittadino	Non inserire i dati della persona nel chatbot; la risposta finale la decide e la firma un essere umano
Selezionare curriculum	Uso ad alto rischio: tocca diritti delle persone e decisioni automatizzate. Richiede valutazioni preventive e supervisione umana

3 AI Act e GDPR

L'AI Act è il regolamento europeo sull'intelligenza artificiale (Regolamento UE 2024/1689), in vigore dal 1° agosto 2024 con un'applicazione graduale nel tempo. **Non sostituisce il GDPR: i due si sommano.**

- **Livelli di rischio** — più il rischio è alto, più le regole sono severe: pratiche vietate, sistemi ad alto rischio, sistemi a rischio limitato con obblighi di trasparenza (ad esempio i chatbot, che devono far capire che si parla con una macchina), sistemi a rischio minimo.
- **I ruoli** — il *fornitore* sviluppa il sistema; il *deployer* lo usa nella propria organizzazione. Enti e aziende sono quasi sempre deployer, con obblighi propri.
- **Le scadenze** — gli obblighi entrano in vigore per fasi e alcune scadenze sono state aggiornate dal legislatore europeo nel 2026: conviene verificare sempre il calendario aggiornato con il proprio DPO.
- **Il rapporto con il GDPR** — se il sistema tratta dati personali valgono entrambe le regole. L'art. 22 GDPR dà diritto a non essere sottoposti a una decisione basata unicamente su un trattamento automatizzato che produca effetti significativi sulla persona.

4 DPIA e FRIA

Due valutazioni con nomi simili e scopi diversi, che si possono integrare in un unico lavoro.

	DPIA	FRIA
Norma	Art. 35 GDPR	Art. 27 AI Act
Cosa valuta	I rischi per i dati personali	I rischi per tutti i diritti fondamentali delle persone

	DPIA	FRIA
Quando	Trattamenti a rischio elevato: tecnologie innovative, valutazioni sistematiche di persone, sorveglianza su larga scala	Prima di mettere in uso un sistema di IA ad alto rischio
Chi la fa	Il Titolare, con il parere del DPO	Il deployer: organismi di diritto pubblico, privati che erogano servizi pubblici, chi usa l'IA per merito creditizio o assicurazioni vita e salute

Quando servono entrambe, la FRIA può completare la DPIA riutilizzando le parti comuni: descrizione del trattamento, rischi, misure. Coinvolgere il DPO anche nella FRIA garantisce coerenza.

Le domande per eseguire la FRIA

Costruite sui sei elementi dell'art. 27 dell'AI Act.

1. **In quali processi sarà usato il sistema, e per quale finalità?**
2. **Per quanto tempo e con quale frequenza sarà usato?**
3. **Quali persone, singole o in gruppo, potrebbero essere toccate dall'uso?**
4. **Quali rischi di danno per i loro diritti fondamentali?**
   Non discriminazione, riservatezza, accesso ai servizi, dignità.
5. **Come è organizzata la supervisione umana?**
   Chi controlla, con quale formazione, con quale potere di intervenire o fermare il sistema.
6. **Quali misure scattano se il rischio si concretizza?**
   Governance interna, canali di reclamo, correzione o sospensione del sistema.

Domande pratiche da aggiungere: chi è il fornitore e quali garanzie offre? Quali dati entrano nel sistema e da dove arrivano? Esiste già una DPIA da riutilizzare? Come si informano le persone coinvolte? Chi aggiorna la valutazione quando il sistema cambia?

5 Dal caso reale al caso pratico

Character.AI, 158.000 euro. Con provvedimento del 3 luglio 2026 il Garante ha sanzionato la società che gestisce il servizio di IA generativa Character.AI. Le contestazioni: informativa carente, DPIA fatta in ritardo, rappresentante nell'UE non designato per tempo, misure di sicurezza e di privacy by design e by default insufficienti, tutela dei minori e verifica dell'età inadeguate. Oltre alla sanzione, l'ordine di adeguarsi entro 120 giorni. La lezione: **la DPIA si fa prima, non dopo.**

Un Comune vuole un chatbot sul sito per rispondere ai cittadini

I passaggi necessari: scelta del fornitore e nomina a Responsabile del trattamento; inserimento nella mappatura; regole d'uso; DPIA ed eventuale FRIA; informativa ai cittadini; indicazione chiara che si sta parlando con una macchina; controllo umano sulle risposte.

Si parte dalla governance, non dallo strumento.

6 Da ricordare

In tre frasi: l'IA è un software fallibile e chi la usa risponde del risultato; servono governance, regole, mappatura e controlli; DPIA e FRIA si fanno prima di mettere in uso un sistema, non dopo.

Prossimo incontro

Venerdì 30 ottobre, 11.15–13.00
Data breach, incidenti di sicurezza e Piano di Sicurezza Informatica

Test finale

Venerdì 30 ottobre, 12.30–13.00, in diretta
15 domande a risposta multipla, si supera con 10 corrette. Superato il test, ricevi l'attestato di partecipazione all'intero ciclo.

oltrecode

Marco La Diega S.r.l. · Via John Kennedy 154, 90031 Belmonte Mezzagno (PA) · Unità locale a Palermo

Sito: www.oltrecode.it · Magazine: oltrecode.it/magazine · Piattaforma GovDPO: www.govdpo.it