TRATTAMENTO DEI DATI PERSONALI CON IA GENERATIVA – Linee guida aggiornate a gennaio 2026

Nel 2026 il trattamento di dati personali tramite sistemi di **IA generativa** è regolato principalmente dal **Regolamento UE 2024/1689 (AI Act)** e, in Italia, dalla **Legge 23 settembre 2025, n. 132** (Disposizioni e deleghe in materia di intelligenza artificiale, in vigore dal 10 ottobre 2025), che integra e specifica l'AI Act a livello nazionale.

Principali scadenze AI Act rilevanti (al gennaio 2026):

- Divieti su certi sistemi e obblighi di literacy AI → dal 2 febbraio 2025
- Obblighi per modelli di IA ad uso generale (GPAI) → dal 2 agosto 2025
- Obblighi di trasparenza (Art. 50) e la maggior parte delle altre disposizioni (inclusi sistemi high-risk) → **dal 2 agosto 2026**

Ecco le informative chiave aggiornate:

1. **Diritti dell'interessato e trasparenza (AI Act – Art. 50 e ss.)**
    - **Obbligo di informare l'utente**: è obbligatorio comunicare chiaramente se si sta interagendo con un sistema di IA e se un contenuto (testo, immagine, audio, video) è generato artificialmente. Per immagini, audio e video generati è richiesto l'uso di **etichette chiare e visibili** (es. watermark digitali o metadata), specialmente per deepfake o contenuti che possono ingannare sul loro carattere sintetico.
    - **Deepfake e contenuti sensibili**: dal 8 gennaio 2026 il **Garante per la protezione dei dati personali** ha emesso un **provvedimento di avvertimento** specifico verso utilizzatori e fornitori di servizi come Grok, ChatGPT e analoghi (es. Clothoff), sottolineando il rischio di gravi violazioni dei diritti fondamentali (privacy, immagine, dignità) in caso di generazione e diffusione di deepfake non consensuali (inclusi casi di "spogliarello digitale" o pornografia non consensuale). L'Autorità si riserva ulteriori misure e collabora con la DPC irlandese per i servizi di X.
2. **Base giuridica e protezione dati (GDPR + AI Act + Legge 132/2025)**
    - **Valutazione d'impatto (DPIA)**: obbligatoria per trattamenti su larga scala, dati sensibili o sistemi classificati ad alto rischio (Art. 35 GDPR + AI Act). Va redatta **prima** dell'uso in produzione.
    - **Principio di minimizzazione**: non inserire mai dati personali sensibili, giudiziari o confidenziali nei prompt di versioni consumer/free. Per usi aziendali/professionali, adottare esclusivamente piani **Enterprise/Business** che includono garanzie contrattuali di **non utilizzo dei dati per addestramento** (no-training clauses).
3. **Focus sulle principali piattaforme (stato al gennaio 2026)**
    - **ChatGPT (OpenAI)**: tra le piattaforme più trasparenti su opt-out. Nelle impostazioni → **Data Controls** → disattivare **"Improve the model for everyone"** (o equivalente). Una volta disattivato, le nuove conversazioni non

vengono usate per addestrare i modelli (resta la cronologia se non disattivata separatamente). Versioni Enterprise garantiscono no-training per default.

- **Grok (xAI)**: **sotto forte attenzione del Garante Privacy italiano**. L'8 gennaio 2026 è stato emesso un **avvertimento formale** per i rischi legati a deepfake non consensuali (immagini generate a partire da foto reali, inclusi contenuti sessualizzati/pedopornografici). Il Garante richiama sia gli utenti (responsabilità penale e civile) sia il fornitore (obbligo di design privacy-by-default). Collaborazione in corso con autorità irlandese; possibili ulteriori provvedimenti.
- **Canva**: la Privacy Policy permette la revisione/uso di contenuti per migliorare i servizi (inclusi modelli AI), salvo opt-out nelle impostazioni privacy o account Team/Enterprise con garanzie rafforzate.
- **Suno** (e tool musicali IA analoghi): obbligo di informativa chiara su diritti di proprietà intellettuale, uso di voci caricate e rischi deepfake vocali. Rientra negli obblighi di trasparenza AI Act; attenzione agli avvertimenti Garante su contenuti generati da input personali.

4. **Responsabilità aziendale e buone pratiche**
   - **Registro delle attività di trattamento** (Art. 30 GDPR): censire **esplicitamente** l'uso di ciascun tool IA (nome, fornitore, finalità, base giuridica, categorie dati, misure di sicurezza).
   - **Accuratezza e non discriminazione**: l'output IA non è esente da errori ("allucinazioni") o bias. L'utente/azienda resta **pienamente responsabile** della verifica e delle decisioni prese sulla base di tali output, specialmente se impattano su persone fisiche (es. assunzioni, valutazioni, profilazioni).
   - **Formazione e policy interna**: prevedere linee guida aziendali sull'uso sicuro di IA generativa, inclusi divieti su dati sensibili e obbligo di verifica output.

Link diretto Garante 8/1/2026: garanteprivacy.it/docweb/-/docweb-display/docweb/10207147.