Checklist GDPR + AI Act

per PMI e Freelance 2026

Cosa deve avere una PMI in regola

con GDPR e AI Act - Aggiornata marzo 2026

5 sezioni | 30+ voci | Rif. normativi

Come usare questa checklist

1. Scorri ogni sezione e spunta le voci gia completate.
2. Le voci non spuntate indicano le priorita su cui agire subito.
3. Ogni voce riporta il riferimento normativo per approfondire.
4. Revisiona la checklist ogni trimestre o quando cambi fornitore o tool AI.

Disclaimer legale

Questa checklist ha finalita orientative per PMI e freelance italiani.

Non sostituisce una consulenza legale, una DPIA formale o il parere di un DPO.

Fonti: GDPR (UE) 2016/679 - AI Act (UE) 2024/1689 - Garante Privacy italiano.

Voce da verificare	*Nota in corsivo = spiegazione del perche*	Riferimento normativo

1 Fondamenta GDPR - Obbligatorio per tutti

Obblighi base che si applicano a qualsiasi PMI o freelance che tratta dati personali, indipendentemente dall'uso di tool AI.

- [ ] **Ho identificato tutti i trattamenti di dati personali in azienda** — artt. 5, 24 e 30 GDPR
  Sapere cosa tratti, perche e come e il punto di partenza di ogni percorso di compliance.
- [ ] **Ho un Registro dei Trattamenti aggiornato** — art. 30 GDPR
  Per le org. con meno di 250 dipendenti esiste un'esenzione limitata, ma il registro resta necessario se i trattamenti non sono occasionali, comportano rischi o includono categorie particolari di dati.
- [ ] **Ho nominato per iscritto ogni fornitore che tratta dati per mio conto** — art. 28 GDPR
  Se un fornitore tratta dati personali per conto del titolare, il rapporto deve essere disciplinato da un contratto o atto giuridico conforme all'art. 28 GDPR.
- [ ] **L'informativa privacy del sito e aggiornata e accessibile** — artt. 13-14 GDPR
  Deve indicare finalita, base giuridica, tempi di conservazione e diritti degli interessati.
- [ ] **Il cookie banner e conforme (consenso granulare, no dark pattern)** — ePrivacy + artt. 4(11), 6-7 GDPR
  Per cookie e strumenti di tracciamento non tecnici serve consenso libero, specifico, informato e documentabile. Il mero scrolling non basta e il legittimo interesse non sostituisce il consenso.
- [ ] **Ho una base giuridica documentata per ogni trattamento principale** — art. 6 GDPR
  Le 6 basi giuridiche GDPR non sono intercambiabili. Il consenso non e sempre la scelta giusta.
- [ ] **I dati personali non sono conservati oltre il necessario (retention policy)** — art. 5(1)(e) GDPR
  Occorre definire e rispettare una retention policy documentata per ogni categoria di dati.
- [ ] **Ho procedure per gestire le richieste degli interessati entro 30 giorni** — artt. 15-22 GDPR
  Accesso, rettifica, cancellazione, opposizione: ogni richiesta deve ricevere risposta scritta nei termini.

2 Tool AI e GDPR - Urgente nel 2025-26

Ogni tool AI che elabora dati personali crea obblighi specifici. Riguarda chi usa ChatGPT, Copilot, Claude, Midjourney o strumenti simili in contesto professionale.

- [ ] **Ho mappato tutti i tool AI usati in azienda, inclusa la Shadow AI** — artt. 5, 24 e 30 GDPR
  L'organizzazione deve governare anche gli usi non autorizzati o non censiti dei tool AI, perche possono generare trattamenti di dati personali sotto la sua sfera organizzativa.
- [ ] **Per ogni tool AI con dati personali, ho verificato termini business e documentazione privacy del provider** — artt. 5, 13-14, 28 GDPR
  Non tutti i piani consumer sono adatti a trattamenti aziendali. Va sempre verificata la documentazione contrattuale e privacy del servizio usato.
- [ ] **Ho verificato se il provider comporta trasferimenti di dati fuori dallo SEE e con quali garanzie** — artt. 44-49 GDPR
  Se i dati sono trasferiti verso paesi terzi, verificare la base applicabile: decisione di adeguatezza, clausole contrattuali standard (SCC) o altra base prevista.

- [ ] **Ho valutato se l'uso di uno o piu tool AI richiede una DPIA**
  La DPIA e necessaria quando il trattamento puo presentare un rischio elevato. La presenza di due o piu criteri di rischio e un forte indicatore, ma occorre valutare anche il contesto concreto e le liste del Garante.
  art. 35 GDPR

- [ ] **L'informativa agli interessati descrive in modo trasparente l'eventuale uso di sistemi AI quando rilevante**
  Se l'AI incide sulle modalita del trattamento, sulla profilazione o sulle decisioni, l'informativa deve spiegare finalita, base giuridica, logica rilevante e diritti dell'interessato.
  artt. 13-14 e 22 GDPR

- [ ] **Ho una policy interna per i dipendenti sull'uso dei tool AI**
  Definisce quali tool sono autorizzati, quali dati si possono inserire e come gestire i prompt con dati personali.
  art. 24 GDPR

- [ ] **Il fornitore AI specifica come usa i dati per addestrare i modelli?**
  Alcuni provider usano i dati degli utenti per il training. Verificare le impostazioni e attivare l'opt-out se disponibile.
  artt. 5, 13-14, 28 GDPR

3 AI Act - Obblighi da verificare secondo la timeline applicabile

L'AI Act ha applicazione graduale: divieti e AI literacy dal 2 febbraio 2025; governance e GPAI dal 2 agosto 2025; applicazione generale dal 2 agosto 2026; sistemi in prodotti regolati dal 2 agosto 2027.

- [ ] **Ho verificato se uso pratiche di AI vietate**
  Le pratiche vietate sono elencate nell'art. 5 AI Act: usi manipolativi, sfruttamento di vulnerabilita, social scoring e alcuni usi biometrici. In vigore dal 2 febbraio 2025.
  art. 5 AI Act

- [ ] **Ho verificato se uso sistemi AI ad alto rischio (Allegato III AI Act)**
  HR (screening CV, valutazione performance), istruzione, infrastrutture critiche: richiedono documentazione, supervisione umana e registrazione specifica.
  art. 6 AI Act

- [ ] **Se utilizzo sistemi AI ad alto rischio, verifico che il provider abbia svolto la procedura di conformita e rilasciato la documentazione richiesta**
  I sistemi AI ad alto rischio devono avere documentazione tecnica e dichiarazione di conformita del provider prima della messa in servizio. Non necessario per sistemi a rischio minimo o limitato.
  art. 47 AI Act

- [ ] **Le persone che usano sistemi AI hanno ricevuto formazione adeguata al ruolo e ai rischi**
  L'AI literacy non e solo formazione introduttiva: deve essere proporzionata ai sistemi usati, al contesto operativo e ai possibili impatti. In vigore dal 2 febbraio 2025.
  art. 4 AI Act

- [ ] **Per sistemi AI ad alto rischio, conservo documentazione, log e controlli coerenti con il mio ruolo**
  Per i sistemi ad alto rischio occorre gestire in modo tracciabile uso, supervisione umana, incidenti e documentazione fornita dal provider.
  artt. 26 ss. AI Act

- [ ] **Ho verificato le scadenze AI Act applicabili al mio settore e ai sistemi che uso**
  Il calendario e graduale: alcune regole gia in vigore, altre dal 2026 o 2027. Verificare la timeline specifica per i sistemi effettivamente usati.
  art. 113 AI Act

4 Contratti e Fornitori AI

La catena contrattuale e tra gli aspetti piu trascurati. Un accordo firmato non basta se le clausole non coprono i rischi reali.

- [ ] **I contratti con i fornitori AI includono clausole su sicurezza e data breach** — art. 28 GDPR
  Il fornitore deve notificarti le violazioni in tempi utili perche tu possa notificare il Garante entro 72 ore.
- [ ] **I contratti specificano i sub-processor del fornitore AI** — art. 28(4) GDPR
  Se il provider usa altri provider (cloud, storage, API), devono essere elencati e coperti da garanzie equivalenti.
- [ ] **Sono chiari i ruoli: titolare / responsabile / contitolare** — art. 26 GDPR
  Alcuni provider AI operano come contitolari per alcune finalita (sicurezza, sviluppo modello). Il ruolo cambia gli obblighi di entrambe le parti.
- [ ] **Il contratto prevede il diritto di audit o di ispezione** — art. 28(3)(h) GDPR
  Il GDPR prevede che il titolare possa verificare il rispetto degli obblighi da parte del responsabile del trattamento.
- [ ] **Il fornitore garantisce la cancellazione dei dati a fine rapporto** — art. 28(3)(g) GDPR
  Alla fine del contratto, i dati personali devono essere cancellati o restituiti. Va previsto esplicitamente.

5 Monitoraggio - Revisione trimestrale

La compliance non e un'azione unica ma un processo continuo. Queste voci vanno riviste ogni trimestre o quando cambiano tool, fornitori o processi.

- [ ] **Revisione trimestrale del Registro dei Trattamenti** — art. 30 GDPR
  Nuovi tool, nuovi fornitori, nuove finalita: il registro deve riflettere la situazione reale e aggiornata.
- [ ] **Aggiornamento delle policy se cambiano tool o fornitori** — art. 24 GDPR
  Ogni volta che si adotta un nuovo tool AI o si cambia fornitore: verifica accordi contrattuali, informativa e policy interna.
- [ ] **Verifica delle nomine contrattuali ancora valide e aggiornate** — art. 28 GDPR
  Gli accordi con i responsabili del trattamento vanno aggiornati se cambiano le condizioni del servizio o le sub-processor list.
- [ ] **Formazione AI Literacy aggiornata per i dipendenti** — art. 4 AI Act
  La formazione deve essere proporzionata ai sistemi usati e ai ruoli. Va aggiornata quando cambiano i tool o le funzioni.
- [ ] **Controllo aggiornamenti normativi (AI Act scadenze, linee guida EDPB)** — Buona prassi
  L'AI Act ha scadenze graduali fino al 2027. Le linee guida EDPB su AI e GDPR si aggiornano regolarmente.
- [ ] **Test periodico delle procedure di risposta ai data breach** — art. 33 GDPR
  Il piano di risposta agli incidenti va testato, non solo scritto. 72 ore sono poche se non si e esercitati.

Prossimi passi

Approfondisci ogni sezione con le guide gratuite su aipolicy.it

Guida GDPR e AI completa	Basi giuridiche, ruoli, DPA e misure minime per PMI	aipolicy.it/guida-gdpr-ai/
AI Act per PMI	Scadenze, obblighi per settore, sistemi ad alto rischio	aipolicy.it/ai-act-pmi/
DPIA per strumenti AI	Quando serve la Valutazione d'Impatto e come farla	aipolicy.it/dpia-strumenti-ai/
Contratti fornitori AI	Cosa verificare prima di firmare con un provider AI	aipolicy.it/contratti-fornitori-ai-clausole/
Mappatura strumenti AI	Come fare l'inventario dei tool AI usati in azienda	aipolicy.it/mappatura-strumenti-ai-azienda/
ChatGPT in azienda e GDPR	Rischi concreti, errori comuni e come mettersi in regola	aipolicy.it/chatgpt-gdpr-aziende-rischi/

Documento aggiornato a marzo 2026. Verifica sempre le ultime linee guida EDPB e i provvedimenti del Garante Privacy italiano. Per trattamenti complessi o dati sensibili, rivolgiti a un DPO o consulente privacy qualificato. Fonti: GDPR (UE) 2016/679 - AI Act (UE) 2024/1689.