skilla

IA in azienda: cosa prevede la normativa italiana

L. 132/2025 e Decreti Attuativi

La guida rapida per

HR · Manager · Persone

Cosa deve fare l'azienda

01 Informare

Comunica al personale quando usi sistemi decisionali o di monitoraggio **integralmente automatizzati** che incidono sul rapporto di lavoro. L'informativa va data **prima dell'avvio del trattamento**.

RIFERIMENTI
- L. 132/2025, art. 11
- D.lgs. 179/2026, art. 41
- D.lgs. 152/1997, art. 1-bis

02 Formare a più livelli

Le norme chiedono di **informare e formare** le persone sui rischi specifici connessi all'uso dell'IA e di sostenere l'**alfabetizzazione** del personale. Un percorso possibile:

- **Tutti:** alfabetizzazione di base sull'IA
- **Chi usa gli strumenti:** uso consapevole e sicuro
- **Chi guida team e decide:** regole, responsabilità, rischi

RIFERIMENTI
- AI Act, art. 4 (come sostituito dal Reg. UE 2026/1744 – Digital Omnibus sull'IA)
- D.lgs. 179/2026, art. 42, c. 3

03 Lasciare la decisione finale a una persona

Le decisioni finali su costituzione, modifica e cessazione del rapporto, compresi provvedimenti disciplinari e valutazioni delle prestazioni, non possono basarsi **solo su un trattamento automatizzato** svolto con i sistemi di IA. **A pena di nullità**, la decisione finale spetta a **una persona con un potere effettivo e autonomo**.

RIFERIMENTI
- D.lgs. 179/2026, art. 41

04 Garantire un uso corretto

Usa strumenti **sicuri, affidabili, trasparenti**, rispettosi di **dignità e privacy** e **privi di discriminazioni**.

RIFERIMENTI
- L. 132/2025, art. 11

05 Aggiornare la valutazione dei rischi

Se l'IA incide su organizzazione del lavoro, ritmi produttivi, modalità di esecuzione della prestazione o processi decisionali rilevanti per la sicurezza, va considerata nella **valutazione dei rischi (DVR)**.

RIFERIMENTI
- D.lgs. 179/2026, art. 42
- D.lgs. 81/2008, art. 28

06 Valutare l'aggiornamento del Modello 231

Per le imprese che lo hanno adottato, servono **presidi** contro la diffusione illecita di immagini, video o voci falsificati o alterati con l'IA, contro l'omessa adozione di misure di sicurezza o di sorveglianza umana sui sistemi di IA ad alto rischio e contro la loro alterazione.

RIFERIMENTI
- D.lgs. 231/2001, art. 25-vicies (introdotto dal D.lgs. 160/2026)

Le tue attenzioni

Non inserire **dati personali o riservati** in strumenti di IA non autorizzati.

RIFERIMENTI
- GDPR, artt. 5 e 32
- policy aziendale

Verifica sempre ciò che l'IA produce: l'IA supporta, ma non sostituisce, la valutazione e la decisione umana.

RIFERIMENTI
- Buona pratica
- L. 132/2025, art. 3, c. 3
- AI Act, art. 26 per i sistemi ad alto rischio (dal 2 dicembre 2027)

Non diffondere contenuti come **immagini, video o voci falsificati o alterati con l'IA** senza il consenso della persona interessata: se causano un danno ingiusto, **è reato**.

RIFERIMENTI
- Codice penale, art. 612-quater (introdotto dalla L. 132/2025)

Usa **solo strumenti approvati** e **segnala anomalie**.

RIFERIMENTI
- Buona pratica
- policy aziendale

Controlli e sanzioni

Chi vigila

- **AgID** — autorità di notifica
- **ACN** — vigilanza del mercato
- **Banca d'Italia, CONSOB e IVASS** — per i sistemi ad alto rischio nei rispettivi settori finanziari
- **Garante privacy** — nei casi previsti dall'AI Act

RIFERIMENTI
- L. 132/2025, art. 20
- D.lgs. 179/2026, artt. 4-5

Quanto si rischia

Responsabilità 231 dell'impresa per la diffusione illecita di immagini, video o voci falsificati o alterati con l'IA e per l'omessa adozione di misure di sicurezza o di sorveglianza umana e l'alterazione dei sistemi ad alto rischio, con **sanzioni pecuniarie e interdittive**

RIFERIMENTI
- D.lgs. 231/2001, art. 25-vicies

Sanzioni penali

Diffusione illecita di immagini, video o voci falsificati con l'IA, con danno ingiusto	1–5 anni
Mancate misure di sicurezza o sorveglianza umana sui sistemi ad alto rischio, con pericolo per le persone (2–8 anni se è in pericolo la sicurezza dello Stato)	1–5 anni
Alterazione illecita dei sistemi ad alto rischio	pene più elevate

Chi usa questi sistemi per lavoro risponde solo se omette intenzionalmente la sorveglianza umana.

RIFERIMENTI
- Codice penale, artt. 612-quater e 437-bis

Pratiche vietate:

fino a
35 milioni €
o al 7% del fatturato mondiale

RIFERIMENTI
- D.lgs. 179/2026, art. 23
- AI Act, art. 99

Altri obblighi, ad esempio quelli di fornitori e deployer:

fino a
15 milioni €
o al 3% del fatturato mondiale
(per i sistemi ad alto rischio dell'Allegato III, gli obblighi si applicano **dal 2 dicembre 2027**)

RIFERIMENTI
- D.lgs. 179/2026, art. 23, c. 2
- AI Act, art. 113 (come modificato dal Reg. UE 2026/1744 – Digital Omnibus sull'IA)

Checklist: da dove partire

Gli step da seguire per dare attuazione alle indicazioni sopracitate

- [ ] 01 **Mappa** gli strumenti di IA in uso, inclusi quelli adottati dai singoli
- [ ] 02 **Classifica** i sistemi per livello di rischio, partendo da quelli che riguardano il personale
- [ ] 03 **Consegna l'informativa** al personale, nei casi previsti
- [ ] 04 **Definisci** chi prende la decisione finale quando l'IA è coinvolta
- [ ] 05 **Aggiorna il DVR** e, se adottato, il **Modello 231**
- [ ] 06 **Adotta una policy interna** sull'uso dell'IA
- [ ] 07 **Avvia la formazione** per tutti i livelli

skilla

Quest'opera è coperta da licenza Creative Commons CC BY NC ND. È pertanto possibile scaricarla e condividerla a condizione che non venga modificata né utilizzata a scopi commerciali e in ogni caso avendo cura di attribuirne la paternità a Skilla - Amicucci Formazione.