

23/09/2026

AI nei software aziendali: le verifiche da fare su dati, contratti e riservatezza

Come valutare una funzione di intelligenza artificiale prima di attivarla in azienda: un metodo per le PMI

Il gestionale si aggiorna nella notte e, la mattina dopo, accanto alle fatture compare un pulsante nuovo: «Riassumi con l'AI». Nel CRM c'è un assistente che sintetizza le conversazioni con i clienti, nella piattaforma paghe un altro propone risposte alle richieste dei dipendenti. Nessuno ha deciso di acquistare un sistema di intelligenza artificiale, eppure in azienda ce n'è già uno.

Succede perché l'AI viene incorporata in software che le imprese usano da anni: gestionali, CRM, piattaforme HR, strumenti cloud, applicazioni di produttività. La domanda utile, allora, non è se vogliamo usare l'AI, ma che cosa deve verificare l'impresa prima di attivare una funzione che ha già a disposizione o che sta per acquistare. Non servono competenze da tecnico: serve sapere che cosa si intende affidare allo strumento e leggere con attenzione ciò che il fornitore garantisce.

Prima del contratto: che cosa entra nello strumento

Il primo passaggio è il più semplice e viene spesso saltato: elencare quali informazioni la funzione andrà a leggere, riassumere o elaborare. Un assistente collegato alla posta tratta i messaggi di clienti e fornitori con i loro allegati; una funzione di analisi documentale legge preventivi e capitolati; una piattaforma HR vede curricula e valutazioni. Conviene ordinare queste informazioni in tre gruppi, perché da lì dipendono le verifiche successive:

- **dati personali** di clienti, dipendenti, candidati, fornitori e altri terzi, con particolare cautela per i dati dei lavoratori e per quelli appartenenti a categorie particolari, come i dati sulla salute;
- **informazioni riservate** dell'impresa e di terzi: preventivi, listini, condizioni commerciali, progetti, file tecnici, procedure interne, documenti ricevuti dai clienti con vincolo di riservatezza;
- **informazioni non sensibili**: testi generici, materiali già pubblici, bozze prive di contenuti riservati.

Molti documenti appartengono a più gruppi insieme. Un'offerta per un cliente contiene il nome del referente (dato personale), prezzi e condizioni che l'impresa non intende diffondere (informazione riservata) e, talvolta, specifiche tecniche che il cliente stesso ha chiesto di non divulgare.

Dati personali, riservatezza e segreti commerciali: tre tutele diverse

È comprensibile pensare che, in assenza di dati personali, non ci sia nulla da controllare. Non è così, perché la protezione dei dati personali, gli obblighi di riservatezza e la tutela dei segreti commerciali seguono strade diverse.

Il GDPR protegge i dati delle persone fisiche. Quando la funzione AI tratta dati di clienti, dipendenti o fornitori entrano in gioco ruoli, informative, misure di sicurezza e il contratto con il fornitore, di cui

parliamo più avanti. Un listino, un preventivo, un disegno costruttivo o una procedura interna non sono invece dati personali, e il GDPR non li protegge per il solo fatto di essere riservati.

La riservatezza di queste informazioni ha altre fonti. La prima è contrattuale: i documenti ricevuti da un cliente o da un committente sono spesso coperti da clausole di riservatezza o da accordi specifici, che vincolano l'impresa anche se nel file non compare alcun dato personale. Caricare quel documento in una funzione AI può significare renderlo accessibile a un soggetto terzo, il fornitore del software, e ciò va confrontato con quanto l'impresa ha pattuito con il cliente.

La seconda è la tutela dei segreti commerciali, disciplinata dagli artt. 98 e 99 del Codice della proprietà industriale. Sono protette le informazioni aziendali e le esperienze tecnico-industriali che siano segrete, cioè non generalmente note né facilmente accessibili agli esperti del settore, che abbiano valore economico proprio perché segrete e che siano sottoposte a misure ragionevolmente adeguate a mantenerle segrete. Quest'ultimo requisito riguarda da vicino chi usa strumenti di AI: il modo in cui l'impresa gestisce un'informazione fa parte delle misure con cui la mantiene segreta. Se le condizioni d'uso consentono al fornitore di riutilizzare i contenuti caricati, o se in azienda chiunque può inserire qualsiasi documento senza regole, sarà più difficile sostenere di aver adottato misure adeguate.

Su questo collegamento non risultano, allo stato delle verifiche effettuate, indicazioni ufficiali specifiche sull'AI: è una lettura prudenziale, non una regola già affermata. Basta però a spiegare perché la classificazione iniziale conta: lo stesso strumento può andare bene per rielaborare testi generici e non andare bene per i documenti dei clienti.

Cosa leggere nel contratto e nelle condizioni d'uso

Le funzioni AI incluse in un software possono essere regolate da condizioni aggiuntive o da aggiornamenti dei termini di servizio che nessuno rilegge, e possono cambiare a seconda della versione del servizio. Vale la pena leggerle una volta, con queste domande.

Che cosa verificare	Domanda da porre al fornitore
Uso dei contenuti	Documenti, email e testi inseriti, e le risposte generate, sono usati per addestrare, migliorare o sviluppare i modelli, del fornitore o di terzi? Si può escluderlo, e vale per tutte le versioni del servizio?
Conservazione	Per quanto tempo restano conservati input, output, cronologia e log? Alla fine del contratto i dati vengono cancellati o restituiti, comprese le copie?
Ruolo privacy	Il fornitore tratta i dati personali per conto dell'impresa, come responsabile del trattamento, con un contratto conforme all'art. 28

GDPR, oppure li usa per finalità proprie?

Subfornitori	Chi altro interviene, ad esempio per il modello o per l'infrastruttura? Esiste un elenco aggiornato e come si viene informati dei cambiamenti?
Localizzazione e trasferimenti	Dove sono trattati i dati e da dove possono essere raggiunti? In caso di trasferimenti fuori dallo Spazio economico europeo, con quale strumento?
Sicurezza e accessi	Come sono gestiti autenticazione, profili, cifratura e registri degli accessi? La funzione rispetta i permessi già presenti nel software o può far emergere contenuti a chi normalmente non li vede? L'amministratore può disattivarla?
Modifiche	Come vengono comunicate le nuove funzioni AI e le variazioni delle condizioni? Si attivano in automatico?

Sul ruolo privacy conviene essere precisi. Quando il fornitore agisce per conto dell'impresa, l'art. 28 GDPR richiede un contratto o un altro atto giuridico che preveda, tra l'altro, il trattamento solo su istruzioni documentate del titolare, l'impegno alla riservatezza delle persone autorizzate, le misure di sicurezza dell'art. 32, la disciplina dei sub-responsabili, la cancellazione o la restituzione dei dati al termine del servizio e la possibilità di verifiche. L'EDPB ha inoltre chiarito, nel parere 22/2024, che il titolare deve avere a disposizione l'identità di responsabili e sub-responsabili: se il fornitore non sa indicarla, è già un'informazione.

Il punto più delicato è l'uso dei dati per migliorare i modelli. Se il fornitore vuole impiegarli per finalità proprie, non è più soltanto una clausola da leggere: l'art. 28, par. 10, prevede che il responsabile che determina finalità e mezzi del trattamento sia considerato titolare, e l'impresa deve chiedersi se e su quale base può consentire quell'utilizzo dei dati di clienti e dipendenti. In questo caso conviene fermarsi e chiedere un parere prima di attivare la funzione.

Chi la usa, per fare che cosa, con quali controlli

Anche il contratto migliore non sostituisce le regole interne. Tre decisioni vanno prese prima dell'attivazione e scritte in poche righe, in un documento che le persone possano davvero consultare.

La prima riguarda **chi può usare la funzione**. Chi ha accesso ai dati personali deve essere istruito dal titolare (artt. 29 e 32, par. 4, GDPR). Attivare un assistente AI per tutti gli utenti del gestionale significa consentire a tutti di sottoporgli qualunque contenuto a cui hanno accesso: spesso è più ragionevole abilitare soltanto i ruoli che ne hanno bisogno.

La seconda riguarda **gli usi consentiti e quelli vietati**. Non serve un elenco lungo: bastano indicazioni chiare, del tipo sì per riformulare comunicazioni commerciali generiche, no per curricula, dati sulla salute, documenti coperti da riservatezza, listini e progetti non ancora divulgati.

La terza riguarda **il controllo umano sugli output**. Il risultato di una funzione AI è una proposta: un riassunto può omettere l'obiezione decisiva di un cliente, una bozza di risposta può promettere ciò che l'azienda non può garantire. Serve una persona con le competenze per verificarlo e la responsabilità di decidere. Quando il risultato riguarda persone, come selezione, valutazione o provvedimenti disciplinari, il controllo deve essere effettivo: l'art. 22 GDPR riconosce il diritto di non essere sottoposti a una decisione basata unicamente su un trattamento automatizzato che produca effetti giuridici o incida in modo analogo significativamente, e il Garante ha ribadito la necessità di un controllo umano in grado di intervenire sul processo decisionale.

Vale anche per la formazione. L'art. 4 dell'AI Act, nella versione modificata dal Regolamento (UE) 2026/1744 in vigore dal 27 luglio 2026, chiede a fornitori e utilizzatori (deployer) di adottare misure per sostenere l'alfabetizzazione in materia di IA di chi usa i sistemi per loro conto, senza imporre, secondo la Commissione europea, un livello specifico. Per una PMI una breve formazione, calibrata sullo strumento e sui dati che tratta, rientra nel metodo.

Tre situazioni concrete

Gli esempi che seguono sono costruiti a scopo illustrativo.

Un software che analizza preventivi e documentazione tecnica. Un'impresa di impianti valuta una funzione che confronta i preventivi dei fornitori e riassume i capitolati. Nei file quasi non ci sono dati personali e viene spontaneo concludere che la privacy non sia un problema. Ma i capitolati sono documenti dei clienti, alcuni soggetti a riservatezza, e i preventivi contengono prezzi e condizioni che costituiscono parte del valore commerciale dell'impresa. Le domande che contano sono altre: le condizioni consentono di usare i documenti per migliorare il modello? Per quanto tempo restano conservati? Quali dipendenti possono caricare quali documenti? Se le risposte non convincono, l'uso può essere limitato ai documenti non riservati.

Un CRM che riassume email e conversazioni con i clienti. La funzione legge messaggi che contengono dati di clienti e dei loro dipendenti, ma anche trattative, condizioni economiche e reclami. Il riassunto salvato nel CRM diventa un nuovo dato, con un proprio tempo di conservazione. Vanno verificati ruolo del fornitore e sub-fornitori, uso dei contenuti per l'addestramento e conservazione dei riassunti, e va deciso chi controlla il riassunto prima che diventi la memoria ufficiale di ciò che il cliente ha chiesto o l'impresa ha promesso.

Un software HR con funzioni AI. La piattaforma propone di analizzare i curricula, sintetizzare le valutazioni dei dipendenti e suggerire chi promuovere. I dati sono personali, riguardano candidati e lavoratori e il rapporto non è paritario. Oltre a ruoli privacy e informative, entrano in gioco le norme sul lavoro: l'informazione ai lavoratori sui sistemi decisionali o di monitoraggio integralmente automatizzati (art. 1-bis D.Lgs. 152/1997, richiamato dall'art. 11 della L. 132/2025) e, se lo strumento consente un controllo a distanza dell'attività, l'art. 4 dello Statuto dei lavoratori, che esclude però gli strumenti usati per rendere la prestazione: la qualificazione va fatta caso per caso. Se le persone

vengono valutate in modo sistematico e su quella base si prendono decisioni, può servire una valutazione d'impatto (art. 35 GDPR).

Il rischio non è teorico. Con un avvertimento del 14 maggio 2026 il Garante ha ritenuto che un plug-in che analizzava con l'AI i messaggi su Slack e Teams per stimare lo stress degli utenti potesse verosimilmente violare la normativa, richiamando la capacità di questi sistemi di generare inferenze ulteriori e chiedendo al fornitore di evitare che i dati degli utenti fossero messi a disposizione dei datori di lavoro, anche in forma di report.

Cosa si applica oggi e cosa arriva dopo

Disciplina	Stato al 20 settembre 2026
GDPR (Reg. UE 2016/679)	Applicabile. Le modifiche proposte dalla Commissione con il Digital Omnibus risultano ancora in discussione.
Segreti commerciali (artt. 98-99 Codice della proprietà industriale)	Applicabili dal 2018. Non esiste una disciplina specifica sull'uso di strumenti AI.
AI Act, art. 4 (alfabetizzazione)	Obbligo già applicabile dal 2 febbraio 2025; nuova formulazione applicabile dal 27 luglio 2026.
AI Act, art. 50 (trasparenza, ad esempio chatbot e contenuti generati)	Applicabile dal 2 agosto 2026; per la marcatura dei contenuti generati da sistemi già sul mercato prima di tale data è previsto un periodo transitorio fino al 2 dicembre 2026.
AI Act, sistemi ad alto rischio (tra cui selezione e valutazione del personale, Allegato III)	Obblighi dal 2 dicembre 2027; per i sistemi integrati in prodotti regolamentati dal 2 agosto 2028.
Lavoro (L. 132/2025, art. 11; D.Lgs. 152/1997, art. 1-bis; L. 300/1970, art. 4)	Già applicabili.

L'AI Act, del resto, non sostituisce le altre regole: la protezione dei dati personali e della riservatezza continua ad applicarsi accanto ad esso (art. 2, par. 7). Il rinvio dell'alto rischio al 2027 non cambia quindi le verifiche descritte in questo articolo, che riguardano norme già in vigore.

In pratica: una scheda per ogni strumento

Per ciascuna funzione AI conviene compilare una scheda di una pagina, con sei informazioni:

1. quali dati e informazioni entrano nello strumento, divisi nei tre gruppi visti sopra;
2. che cosa prevedono contratto e condizioni d'uso su addestramento, conservazione, subfornitori e trasferimenti;

3. quale ruolo ha il fornitore ai fini privacy e se serve la nomina a responsabile;
4. quali misure di sicurezza e quali profili di accesso sono previsti;
5. chi può usarlo e per quali attività, con gli usi vietati;
6. chi verifica gli output e come.

L'esito può essere uno di tre: attivare, attivare con limiti (certi utenti, certe categorie di documenti) oppure non attivare, o rinviare, finché il fornitore non ha risposto alle domande aperte.

Dentro i processi che già esistono

La scheda non è un nuovo adempimento e non richiede un comitato. Le sue domande sono già quelle che un'impresa ordinata si pone quando sceglie un software o cambia fornitore: quanto costa, chi offre assistenza, dove stanno i dati, chi vi accede. L'AI ne aggiunge poche a un processo che c'è già.

Nella scelta di un nuovo software, o al rinnovo di un contratto, le domande sull'AI entrano nella richiesta di offerta e nella valutazione del fornitore. Sul piano privacy, se la funzione tratta dati personali si aggiornano nomine, informative e registro dei trattamenti e si valuta se serva una valutazione d'impatto. Sul piano della sicurezza, chi gestisce gli accessi decide quali profili abilitare. Sul piano organizzativo, le regole d'uso si affiancano a quelle che l'impresa ha già per posta elettronica, dispositivi e servizi cloud.

Rimane il caso di chi i software li ha già, perché l'AI arriva con gli aggiornamenti. Per ciascun software conviene stabilire chi riceve le comunicazioni del fornitore e chi decide se, quando e per chi una nuova funzione viene attivata. La valutazione resta proporzionata: una funzione che rielabora testi senza dati riservati richiede pochi controlli, una che legge tutte le email dei clienti richiede la scheda completa.

Lo sguardo della professionista

Patrizia Venuti – Dottore Commercialista e Revisore Legale

Nella consulenza alle PMI su organizzazione e uso consapevole dell'AI, il punto che considero decisivo è chi decide. Un contratto ben letto serve a poco se in azienda nessuno ha il compito di stabilire che una funzione può essere attivata, da chi e su quali documenti: è questa assenza, più di una clausola sfavorevole, a lasciare la decisione al primo dipendente che preme il pulsante.

Per questo suggerisco di partire dal processo e non dallo strumento: individuare le attività in cui l'AI può servire davvero e le informazioni che quelle attività toccano. Da lì la valutazione diventa proporzionata, con pochi controlli dove i dati sono banali e verifiche complete dove passano documenti dei clienti, dati dei dipendenti o know-how dell'impresa.

Il risultato da ottenere è semplice: quando qualcuno usa la funzione, l'impresa sa già che cosa accade alle informazioni che ha inserito.

Riferimenti

Regolamento (UE) 2016/679 (GDPR), artt. 22, 28, 29, 32 e 35.

Regolamento (UE) 2024/1689 (AI Act), artt. 2, par. 7, 4, 50, 113 e Allegato III, punto 4, come modificato dal Regolamento (UE) 2026/1744 (Digital Omnibus sull'IA), pubblicato nella Gazzetta ufficiale dell'Unione europea del 24 luglio 2026 e in vigore dal 27 luglio 2026: alto rischio (Allegato III) dal 2 dicembre 2027.

Commissione europea, AI Literacy – Questions & Answers (aggiornamento 27 luglio 2026).

D.Lgs. 10 febbraio 2005, n. 30 (Codice della proprietà industriale), artt. 98 e 99, come modificati dal D.Lgs. 11 maggio 2018, n. 63 (attuazione della direttiva (UE) 2016/943 sui segreti commerciali).

Legge 23 settembre 2025, n. 132, art. 11; D.Lgs. 26 maggio 1997, n. 152, art. 1-bis; Legge 20 maggio 1970, n. 300, art. 4.

EDPB, Parere 22/2024 su taluni obblighi derivanti dal ricorso a responsabili e sub-responsabili del trattamento (9 ottobre 2024).

Garante per la protezione dei dati personali, provvedimento del 14 maggio 2026, avvertimento nei confronti di Myndoor S.r.l. [doc. web n. 10255494].

Patrizia Venuti – Dottore Commercialista e Revisore Legale