

Usare l'intelligenza artificiale in modo sicuro e responsabile

Un dato inviato non si ritira. L'assistente propone, una persona decide.

CONCETTI CHIAVE

Shadow AI (IA «nell'ombra»)

Usare per lavoro strumenti non autorizzati o account personali. Valgono condizioni pensate per i privati e l'organizzazione non ha controllo su dati, conservazione e accessi. Non basta l'email di lavoro: un piano per privati attivato con quell'indirizzo resta un account personale; l'account di lavoro è gestito dall'organizzazione e coperto dal suo contratto con il fornitore. Anche con un account personale, l'uso per lavoro di norma rientra nelle regole dell'organizzazione. Chi lavora in proprio sceglie piani professionali e, se usa dati personali dei clienti, stipula con il fornitore un accordo sul trattamento dei dati (art. 28 GDPR).

Informazioni da proteggere

Mai le credenziali. Dati personali, dati di clienti e fornitori, informazioni commerciali riservate, documenti coperti da accordi di riservatezza (NDA) e informazioni di sicurezza: solo se è espressamente previsto, dall'organizzazione o, per chi lavora in proprio, dagli accordi con i clienti. Test: ciò che non si condividerebbe con uno studio di consulenza esterno, vincolato alla riservatezza, non va nemmeno nell'assistente; se lo si condividerebbe, valgono comunque le regole sugli strumenti autorizzati e sui dati personali.

Allucinazioni

Risposte inventate ma scritte in modo convincente: sentenze, leggi e fonti inesistenti, articoli sbagliati, numeri plausibili ma falsi, citazioni attribuite a persone reali. Il tono sicuro non è una prova: le fonti si controllano sull'originale.

Verifica e responsabilità

Fatti e numeri · fonti · norme e date · tono e contesto · «lo firmerei?». Il controllo è proporzionato all'uso del risultato. L'assistente propone, una persona decide: verso l'esterno ne risponde di regola l'organizzazione, o chi lavora in proprio. Chi svolge una professione intellettuale informa i clienti su quali sistemi di IA usa (L. 132/2025, art. 13).

Il percorso dei dati

Con i servizi in cloud, il prompt, cioè la richiesta scritta all'assistente, e gli allegati vengono elaborati sui server del fornitore, che possono trovarsi anche fuori dall'UE, e possono esservi conservati. Sui piani per privati possono servire ad addestrare i modelli. Un dato inviato non si ritira: cancellare la chat non annulla l'invio. Se finisce nell'assistente qualcosa che doveva restare fuori, lo si segnala subito a chi coordina il lavoro o al referente privacy.

Dati personali e GDPR

Un prompt con dati personali è un trattamento: base giuridica e finalità le valuta l'organizzazione, o chi lavora in proprio. Solo i dati indispensabili, con sigle o ruoli al posto dei nomi: riducono il rischio, ma non rendono i dati anonimi. Come regola operativa, niente categorie particolari (salute, opinioni politiche, convinzioni religiose, appartenenza sindacale, dati biometrici e simili, oltre ai dati su condanne penali), salvo procedure specifiche dell'organizzazione o, per chi lavora in proprio, una valutazione specifica. Nel dubbio, il responsabile della protezione dei dati (DPO) o il referente privacy.

Gli altri limiti

Distorsioni (bias), conoscenze non aggiornate, fiducia eccessiva nell'automazione, istruzioni nascoste in documenti e pagine web (prompt injection).

Diritto d'autore

Caricare opere di terzi solo se la licenza o le condizioni d'uso lo consentono; controllare che gli output non riproducano opere protette. Le opere create con l'ausilio dell'IA sono tutelate solo se hanno carattere creativo e sono il risultato del lavoro intellettuale dell'autore (L. 132/2025, art. 25).

SETTE REGOLE OPERATIVE

1. Usare solo strumenti autorizzati, con l'account di lavoro.
2. Mai credenziali; dati personali e informazioni riservate solo se è espressamente previsto.
3. Ridurre i dati al minimo e sostituire i nomi con sigle o ruoli, sapendo che non rendono i dati anonimi.
4. Verificare fatti, numeri, fonti e norme prima di usare un risultato.
5. Caricare materiale di terzi solo se la licenza o le condizioni d'uso lo consentono.
6. Con documenti e pagine esterne, controllare che cosa fa l'assistente: possono contenere istruzioni nascoste.
7. Nel dubbio, chiedere prima; se qualcosa va storto, segnalarlo subito: a chi coordina il proprio lavoro, al DPO o, se c'è, al referente per l'IA.