CORSO BASE · LEZIONE 2 DI 3

Usare l’intelligenza artificiale in modo sicuro e responsabile

Strumenti autorizzati, dati da proteggere, limiti dell’IA e verifica dei risultati

AI Act per chi usa l’intelligenza artificiale al lavoro — Lucio Buricca

Presentatrice e voce generate con intelligenza artificiale; testi preparati con il supporto di strumenti di IA e verificati dall’autore. Contenuto informativo aggiornato a settembre 2026; non costituisce consulenza legale.

Strumenti autorizzati e account personali

Strumento autorizzato

- Scelto e configurato dall’organizzazione
- Contratto con il fornitore: riservatezza e uso dei dati definiti
- Account di lavoro, gestito dall’organizzazione
- Uso conforme alla policy interna

Strumenti non autorizzati (shadow AI)

- Spesso con un account personale, anche con l’email di lavoro
- Condizioni pensate per l’uso privato
- I dati possono servire ad addestrare i modelli
- L’organizzazione non controlla conservazione e accessi
- L’organizzazione non sa che cosa è stato inserito

Per il lavoro si usano solo gli strumenti autorizzati, con l’account di lavoro. Chi lavora in proprio sceglie piani professionali e, se tratta dati personali dei clienti, un accordo sul trattamento dei dati.

Che cosa accade ai dati inseriti



Con i servizi in cloud, ogni richiesta esce dal proprio computer: testo e allegati vengono elaborati sui sistemi del fornitore, secondo le sue condizioni.

Piani per privati: possibile uso per addestrare i modelli

Server anche fuori dall'UE: trasferimento di dati personali, ammesso solo alle condizioni del GDPR

Piani aziendali: uso dei dati regolato dal contratto

Una volta inviato, un dato non si ritira: cancellare la conversazione non annulla l'invio.

Informazioni da proteggere

Dati personali

Dati del personale, della clientela, di persone identificabili.

Dati di clienti e fornitori

Contratti e informazioni ricevute in via riservata.

Informazioni commerciali riservate

Prezzi, margini, strategie, progetti non pubblici.

Credenziali

Password, codici di accesso, chiavi di sistema.

Documenti sotto NDA

Materiale coperto da accordi di riservatezza.

Informazioni di sicurezza

Configurazioni, vulnerabilità, procedure di sicurezza.

Credenziali mai; il resto solo se è espressamente previsto. Test: lo si condividerebbe con uno studio di consulenza esterno vincolato alla riservatezza? Se no, non va nell’assistente.

Dati personali e GDPR

Dati personali nel prompt: è un trattamento

Inserire dati personali in un assistente è un trattamento di dati ai sensi del GDPR.

Base giuridica e finalità

Base giuridica e finalità compatibili: le valuta l'organizzazione; chi lavora segue le istruzioni ricevute.

Minimizzare e pseudonimizzare

Solo i dati indispensabili; nomi sostituiti da sigle o ruoli. Le sigle riducono il rischio, ma non rendono i dati anonimi.

Niente categorie particolari

Salute, opinioni politiche, convinzioni religiose, appartenenza sindacale, dati biometrici e simili, oltre ai dati su condanne penali: restano fuori, salvo procedure specifiche.

Nel dubbio, prima di inserire dati personali, ci si rivolge al responsabile della protezione dei dati (DPO) o al referente privacy.

Allucinazioni: il falso che sembra vero

Mi citi una sentenza della Cassazione sull'IA per valutare il personale?

Esempio di risposta inventata

Certo. Con la sentenza n. 4521 del 31 aprile 2021, la Cassazione, sezione lavoro, ha stabilito che ogni valutazione fatta con l'IA deve essere rivista da un dirigente entro trenta giorni.

INVENTATA

Le forme più comuni

- Sentenze, leggi e fonti inesistenti
- Articoli di legge sbagliati o superati
- Numeri e dati plausibili ma falsi
- Citazioni attribuite a persone reali

Il 31 aprile non esiste: sentenza e regola sono inventate. Il tono sicuro non è una prova: le fonti si controllano sull'originale.

Gli altri limiti da conoscere

Distorsioni (bias)

Il modello può riflettere squilibri e stereotipi presenti nei dati di addestramento.

Conoscenze non aggiornate

Norme, prezzi e fatti recenti possono mancare o essere superati.

Fiducia eccessiva nell'automazione

Più lo strumento sembra affidabile, più si tende a smettere di controllare.

Istruzioni nascoste

Documenti e pagine web possono contenere comandi che deviano l'assistente.

Nessuno di questi limiti si vede a colpo d'occhio: per questo serve un metodo di verifica.

La verifica umana in cinque passi

1

Fatti e numeri

Controllare dati, calcoli, nomi e date.

2

Fonti

Verificare che esistano e dicano davvero ciò che si afferma.

3

Norme e date

Controllare articoli e scadenze sul testo ufficiale aggiornato.

4

Tono e contesto

Adattare il testo a chi lo riceve e alla situazione.

5

«Lo firmerei?»

Se non si è disposti a firmarlo con il proprio nome, non è pronto.

La verifica è proporzionata all’uso: una bozza interna richiede meno controlli di un documento per un cliente o di un parere.

Chi risponde del risultato

L’assistente propone, una persona decide: la responsabilità non passa allo strumento.



Decide una persona

Usare, firmare o inviare un testo è una scelta di chi lo fa, secondo le regole del proprio contesto di lavoro.



Verso l’esterno

Con clienti e terzi ne risponde di regola l’organizzazione, o chi lavora in proprio: non lo strumento.



Dichiararlo quando serve

Se l’uso dell’IA conta per chi riceve il lavoro. Chi svolge una professione intellettuale informa i clienti su quali sistemi di IA usa (L. 132/2025, art. 13).

Diritto d’autore e contenuti di terzi

Non caricare opere di terzi

Testi, immagini e documenti protetti di altri: solo se la licenza o le condizioni d’uso lo consentono.

Risultati da controllare

Un risultato può riprodurre opere protette: va controllato prima di pubblicarlo.

Opere create con l’ausilio dell’IA

Tutelate solo se creative e frutto del lavoro intellettuale dell’autore (L. 132/2025).

Prima di pubblicare testi o immagini generati, si controlla che non riproducano opere altrui e che l’uso rispetti le regole del proprio contesto di lavoro.

IN SINTESI

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.

Dove esiste, la policy della propria organizzazione fissa le regole di dettaglio: questo corso non la sostituisce.

AUTOVERIFICA

Tre domande per fissare quanto visto

D1

Chi lavora come dipendente riassume il contratto di un cliente con il proprio account personale. Il problema?

A) dati riservati finiti fuori dagli strumenti autorizzati · B) nessuno, se il testo è giusto · C) nessuno, se poi cancella la chat

D2

Un assistente cita una sentenza con numero e data. Che cosa si fa?

A) la si usa: i dettagli la rendono affidabile · B) si chiede all'assistente se è vera · C) la si verifica sulla fonte ufficiale

D3

Lo strumento autorizzato consente dati personali e il compito li richiede. Come si procede?

A) si inserisce tutto, per completezza · B) solo il necessario, con sigle o ruoli dove possibile · C) nessun limite: è autorizzato

Le risposte sono nella slide successiva.

AUTOVERIFICA

Le risposte

D1 — **Chi lavora come dipendente riassume il contratto di un cliente con il proprio account personale. Il problema?**

✓ **A) dati riservati finiti fuori dagli strumenti autorizzati** · B) nessuno, se il testo è giusto · C) nessuno, se poi cancella la chat

D2 — **Un assistente cita una sentenza con numero e data. Che cosa si fa?**

A) la si usa: i dettagli la rendono affidabile · B) si chiede all'assistente se è vera · ✓ **C) la si verifica sulla fonte ufficiale**

D3 — **Lo strumento autorizzato consente dati personali e il compito li richiede. Come si procede?**

A) si inserisce tutto, per completezza · ✓ **B) solo il necessario, con sigle o ruoli dove possibile** · C) nessun limite: è autorizzato

Le risposte corrette sono evidenziate in verde.

FINE DELLA LEZIONE 2

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

PROSSIMA LEZIONE

Lezione 3 — Dove passano i confini: divieti, decisioni sulle persone e trasparenza

Presentatrice e voce generate con intelligenza artificiale; testi preparati con il supporto di strumenti di IA e verificati dall’autore. Contenuto informativo aggiornato a settembre 2026; non costituisce consulenza legale.