AGENZIA WEB MONZA / GUIDA 03

Database e gestione dei dati per agenti AI

Database, contesto RAG, riservatezza, provider AI e responsabilità sul trattamento.

Dati sotto controllo

Documento informativo e commerciale • Ottobre 2026

Non costituisce preventivo, contratto o garanzia di conformità normativa.

Il database è la memoria operativa, non il modello AI

Il sistema deve distinguere i dati verificati dall'azienda dalle risposte generate dal modello. Clienti, ordini, commesse, pratiche, autorizzazioni e documenti appartengono ai sistemi dati controllati; l'AI li consulta nei limiti concessi e può produrre proposte, mai sostituire automaticamente la fonte ufficiale.

> **L'AI interpreta e propone. Il database conserva dati strutturati e verificabili. Il backend applica le regole.**

Come organizziamo le informazioni

Anagrafiche, prodotti e commesse

Un'attività produttiva può avere tabelle e sistemi per clienti, prodotti, distinte materiali, ordini, commesse e movimentazioni. Ogni operazione deve mantenere riferimenti e stati coerenti, con validazioni e transazioni quando necessarie.

Professionisti e pratiche

In uno studio vengono distinti utenti, clienti, pratiche, documenti, eventi e comunicazioni. Le autorizzazioni devono essere applicate alle singole informazioni, non soltanto alla pagina visibile.

Dati prodotti dall'AI

Le bozze e le proposte generate devono essere marcate come tali, con stato di verifica, fonte dei dati usati e, se necessario, identificativo del responsabile che ha approvato.

RAG: consultare documenti senza addestrare un modello

La Retrieval-Augmented Generation (RAG) permette di recuperare estratti pertinenti da documenti e usarli come contesto. Non equivale automaticamente all'addestramento del modello. I documenti possono essere indicizzati tramite embeddings e un archivio vettoriale, ma questo non elimina i rischi privacy o di divulgazione.

- Ogni frammento deve mantenere proprietario, identificatore del documento, versione e permessi.
- Prima e dopo la ricerca si verificano le autorizzazioni: filtrare dopo aver mostrato dati al modello può essere troppo tardi.
- I documenti aggiornati o cancellati devono avere un processo di sincronizzazione con indice e cache.
- Gli embeddings e i metadati possono essere personali o rivelare informazioni riservate: vanno protetti.
- Le fonti devono essere tracciabili per consentire verifica delle risposte.

Separazione fra aziende e clienti

In sistemi multi-azienda un errore di filtro può mostrare informazioni di un cliente a un altro. I controlli devono essere realizzati nel backend e, quando disponibile, rafforzati da policy a livello database (ad esempio Row Level Security), con test automatici di isolamento.

Un agente non deve avere un’unica credenziale di amministratore per cercare indistintamente tra tutte le pratiche. Occorrono identità di servizio limitate, token a breve durata ove appropriato e registrazione delle azioni sensibili.

Inviare dati a un provider AI: cosa cambia

I dati inviati a un’API esterna possono comprendere richieste, estratti documentali, metadati e istruzioni. Prima dell’integrazione vanno verificati: termini del fornitore, ruoli privacy, sottofornitori, localizzazione dei trattamenti, conservazione di input/output, eventuale uso per training, misure di sicurezza e condizioni di trasferimento internazionale.

Non si deve presumere che i dati siano residenti in UE, che non siano conservati o che non vengano utilizzati per addestramento: queste condizioni dipendono dal provider, dal prodotto e dalle impostazioni contrattuali effettive.

Si applica la minimizzazione: inviare solo dati realmente necessari, possibilmente pseudonimizzati quando utile. Il consenso non è automaticamente l’unica o la corretta base giuridica: dipende dalla finalità.

Conservazione, cancellazione e backup

- Definire tempi di conservazione distinti per anagrafiche, pratiche, ordini, log, documenti e bozze AI.
- Gestire cancellazioni e richieste dell’interessato tenendo conto di obblighi legali di conservazione.
- Proteggere backup e copie di ripristino, con procedure di cancellazione o scadenza coerenti.
- Mantenere registrazioni tecniche necessarie a ricostruire eventi evitando log di prompt integrali non necessari.
- Prevedere esportabilità: dati strutturati, file allegati, mapping dei record e documentazione delle integrazioni.

Il fatto che hosting o database siano intestati al cliente non determina da solo ruoli GDPR, proprietà intellettuale o tutte le responsabilità: occorrono accordi e valutazioni coerenti.

Normative applicabili: impostazione pratica

GDPR

Verificare principi art. 5 (finalità, minimizzazione, esattezza, conservazione), sicurezza art. 32, rapporti con responsabili art. 28, trasferimenti internazionali e DPIA art. 35 quando richiesta. L’informativa deve descrivere correttamente l’uso dei dati e l’eventuale coinvolgimento di servizi AI.

AI Act

La disciplina applicabile dipende dalla funzione dell’agente. L’uso per supporto amministrativo generico non va automaticamente equiparato a un sistema ad alto rischio; applicazioni in ambiti regolati o destinate a decisioni che incidono su persone richiedono analisi di classificazione specifica, tenendo conto delle disposizioni applicabili nel tempo.

Segreto professionale e riservatezza

Oltre al GDPR possono applicarsi obblighi professionali, contrattuali o settoriali di riservatezza. Occorre decidere quali documenti non possano uscire dall’infrastruttura controllata e se sia opportuno usare un

modello locale o una configurazione dedicata.

Esempio di ciclo completo: richiesta di aggiornamento pratica

- 1. L’utente viene autenticato; il backend verifica l’accesso alla pratica.
- 2. Vengono selezionati solo stato e documenti rilevanti e autorizzati.
- 3. Il motore di ricerca contestuale produce fonti e riferimenti.
- 4. Il modello genera una bozza, con indicazione delle informazioni mancanti.
- 5. Il professionista approva; il software registra il passaggio e invia il messaggio.
- 6. Log, dati temporanei e file vengono conservati secondo regole definite.

> **Il contesto dell’AI deve essere limitato alla persona, alla pratica e allo scopo corretti.**

Checklist di consegna e controllo dei dati

- Schema dei dati e mappa dei sistemi collegati.
- Elenco dei fornitori e delle tipologie di dati trasmesse.
- Matrice dei permessi e ruoli degli utenti.
- Policy di retention, backup, esportazione e cancellazione.
- Verifica contrattuale e privacy del fornitore AI, comprese condizioni su training e localizzazione.
- Test documentato di isolamento tra clienti e di recupero dei dati.

L’infrastruttura viene progettata per dare al cliente il controllo delle risorse concordate, compresi dominio e hosting intestati al cliente; la realizzazione effettiva e i costi dipendono dall’architettura definita.

Riferimenti per approfondire

Commissione UE - AI Act, calendario e FAQ - https://ai-act-service-desk.ec.europa.eu/en/ai-act/eu-ai-act-implementation-timeline

EDPB - accountability e ruoli GDPR - https://www.edpb.europa.eu/topics/accountability-and-compliance-tools/accountability_en

OWASP - Top 10 per applicazioni LLM - https://genai.owasp.org/llm-top-10/

Nota: documento informativo e commerciale, non contrattuale e non sostitutivo di consulenza legale, fiscale o di una valutazione privacy e sicurezza sul progetto specifico. Funzionalità, misure, importi e responsabilità saranno definite nel preventivo e negli accordi applicabili. Aggiornato a ottobre 2026.