JJ5.2 - Tetto di spesa e riservatezza

In una frase. L'assistente ha un tetto di spesa al giorno e regole precise su quali dati possono arrivare al servizio di intelligenza artificiale.

Ogni domanda costa qualcosa, perché usa un servizio esterno a pagamento. E ogni domanda manda fuori un po' di testo. Chi amministra deve poter rispondere a due domande: quanto si spende al massimo, e cosa esce.

Il tetto di spesa. L'assistente registra per ogni domanda modello, consumo, costo e durata. Prima di ogni nuova domanda somma la spesa del giorno: se ha raggiunto il tetto, non parte e la chat dice «Per oggi è stato raggiunto il tetto di spesa: riprova domani o chiedi di alzarlo». Il tetto predefinito è 5 dollari al giorno. C'è anche un limite di lavoro per singola domanda e un numero massimo di domande insieme.

Cosa esce verso il modello.

- La domanda, così come l'hai scritta.
- I significati del catalogo: nomi di tavole e colonne, regole.
- Un'anteprima dei risultati delle ricerche sui Dati spiegati: le prime righe.

Cosa non esce.

- I Dati aziendali: il modello non li vede e l'assistente non li legge.
- Dati di persone: i Dati spiegati sono pensati senza email, telefoni e indirizzi.

Dove sta il modello. La regola di ADSWnext per i dati dei clienti è: intelligenza artificiale spenta in partenza, e solo fornitori nell'Unione europea. L'assistente dichiara alla chat, prima di ogni invio, quale servizio usa e in quale regione: se non risponde, la chat non invia.

> **Attenzione.** Oggi l'assistente gira solo nell'ambiente di prova interno, con dati fittizi, e lì usa un instradamento non garantito nell'Unione europea: la chat lo dichiara. Prima di usarlo con i dati di un cliente vanno chiuse due cose: passare all'instradamento europeo e decidere come trattare i nomi scritti nelle domande, che oggi partono senza essere sostituiti.

> **Nota.** L'assistente che nel catalogo aiuta a preparare le proposte ha un tetto di spesa suo, separato.

>

Per chi sviluppa. Tetto: `SIGEAGENT_TETTO_SPESA_GIORNALIERO_USD`. Instradamento europeo: l'impostazione `OPENROUTER_BASE_URL` del servizio va portata a `https://eu.openrouter.ai/api/v1`; il compose di deploy oggi non la passa. La dichiarazione del fornitore è l'endpoint `/ai/agent/fornitore` in `backend/middleware/sigeagent/src/sigeagent/web.py`. Regole generali e l'eccezione dell'assistente: `docs/ai/AI-CONFORMITA.md`.

Per approfondire.
• Informativa sull'intelligenza artificiale per il cliente: `docs/ai/INFORMATIVA-AI-CLIENTE.md`

Revisione #2
Creato 17 novembre 2026 07:58:34 da Giuseppe Anelli
Aggiornato 17 novembre 2026 09:37:41 da Genesys Software