

Loquimini chat Multilingua

"Loquimini - Chat Multilingua Effimera On-Premise per la PA"

Analisi di Impatto, Minimizzazione dei Dati, Sicurezza e Sostenibilità Economica

1. Architettura tecnica

Il sistema Loquimini è integralmente auto-ospitato presso l'infrastruttura dell'Ente ed è basato su:

- Sistema operativo Debian 13 su VM o bare metal
- Linguaggi php8.4 javascript python
- Webapp dedicata installata su dispositivi istituzionali
- Comunicazioni cifrate tramite TLS (HTTPS)
- Chat verso chiunque tramite invio link Qrcode anonimo senza registrazione o installazione
- Trasferimento documenti in sessione effimera senza conservazione.
- Invio messaggi audio diretti o tradotti
- Videochiamate (sistema interno nessun servizio esterno)

Tutti i componenti utilizzati sono open source da Debian repository, Vanilla.

1.2 Modalità di funzionamento

- Ogni sessione di chat viene eseguita all'interno di un'istanza volatile e isolata del sistema
- A ciascuna sessione è associata una cartella temporanea randomizzata
- Al termine della sessione:
 - la cartella viene distrutta automaticamente
 - i dati transitori vengono eliminati
 - nessun contenuto viene archiviato o conservato
- Sistema traduzione basato su Sistema llama.cpp modello AI interno o argostranlate

2 Flusso dati

- I messaggi sono scambiati esclusivamente durante la sessione attiva
- I contenuti non sono salvati su database o file system persistenti
- I file eventualmente condivisi sono disponibili solo fino alla chiusura della sessione
- Nessun dato è trasferito verso infrastrutture di terzi o Paesi extra-UE

2.1 Dati personali Privacy

Il sistema non richiede né conserva dati personali persistenti.

Durante la sessione possono transitare:

- Testi inseriti volontariamente dagli utenti
- File o documenti condivisi temporaneamente
- Indirizzo IP, limitatamente alle esigenze tecniche di comunicazione
- Nessuna registrazione con numero di telefono o qualsiasi dato personale

Non sono trattati dati particolari ex art. 9 GDPR.

3. Analisi dei Rischi e Misure di Mitigazione

Poiché il sistema non richiede né conserva dati personali persistenti (trattando solo testi transitori, file temporanei e IP per esigenze tecniche, senza dati particolari ex art. 9 GDPR), i rischi risultano limitati temporalmente alla durata della sessione:

Vettore di Rischio	Misura di Mitigazione Adottata	Mitigazione Rischio Residuo
Intercettazione del traffico	TLS completo e infrastruttura server on-premise.	Adeguate
Accesso non autorizzato	Link randomizzati e sessioni monouso / QR code.	Alta
Esfiltrazione / Fuga di dati	Assenza di persistenza, distruzione automatica post-sessione.	Molto alta
Errore di configurazione	Uso di Virtualmin, formazione tecnica e documentazione dedicata.	Adeguate
Errore utente (dati inseriti)	Natura anonima delle sessioni e applicazione rigorosa della minimizzazione.	Adeguate

4. Confronto con Soluzioni Commerciali Esterne

Il sistema supera nettamente le criticità di piattaforme commerciali di terze parti (quali WhatsApp, Telegram, WeChat o Google Translate) in termini di localizzazione dei dati (interamente nell'infrastruttura PA), assenza di tracciamento telefonico, conformità alla Privacy by Design e totale indipendenza da vendor esteri [cite: 9].

5. Modello Economico e Sostenibilità del Trattamento

Il sistema adotta un modello economico coerente con i principi di economicità, trasparenza e proporzionalità della PA (art. 97 Cost., art. 1 L. 241/1990) [cite: 9]:

- Solo costo installazione fornito con licenza apache 2