

DPIA – Valutazione d’Impatto sulla Protezione dei Dati

Sistema: Loquimini – Chat multilingua effimera per la PA

Versione: 1.0

Redatto per: Pubblica Amministrazione richiedente

1. Introduzione

La presente valutazione d’impatto è redatta ai sensi dell’art. 35 GDPR, al fine di analizzare i rischi sulla protezione dei dati connessi all’uso del sistema **Loquimini**, piattaforma di comunicazione multilingua basata su chat temporanee (“usa e getta”), installata on-premise presso la PA.

2. Descrizione del trattamento

2.1 Finalità del sistema

- Facilitare la comunicazione tra PA e cittadini (italiani o stranieri) tramite chat in tempo reale.
- Consentire traduzione multilingua automatica durante la conversazione.
- Garantire modalità **privacy-by-design**, con assenza di conservazione dei contenuti scambiati.

2.2 Funzionamento sintetico

- Installazione on-premise su server della PA (Debian 13 + Virtualmin).
- Ogni sessione chat viene eseguita in una **copia volatile del programma**, con cartella temporanea randomizzata.
- Al termine della sessione:
 - viene distrutta la cartella,
 - vengono eliminati i dati transitori,
 - nessun contenuto viene archiviato.

2.3 Tipologia di utenti

- **Utenti istituzionali interno PA:** accesso tramite link con *identificativo random/hash*, senza dati personali, credenziali minime pseudonimizzate.
- **Cittadini:** link monouso o QR code che genera una sessione anonima.

2.4 Dati trattati

Il sistema *non* richiede né trattiene dati personali persistenti. I dati “in transito” possono includere:

- Testi dei messaggi inviati volontariamente dall'utente.
- File e documenti inviati durante la sessione (disponibili solo fino alla chiusura).
- Indirizzo IP (tecnicamente necessario alla comunicazione).

2.5 Soggetti coinvolti

- **Titolare del trattamento:** PA.
- **Amministratori titolari dell'infrastruttura:** tecnici PA.
- **Fornitore (Loquimini):** ruolo limitato a *installazione, formazione, supporto*; nessun accesso ai dati in produzione.

2.6 Tecnologie utilizzate

- Server Debian 13 con Virtualmin (open source).
 - WebApp installata sui device istituzionali.
 - Cifratura TLS (HTTPS).
 - Eliminazione automatizzata dei dati a fine sessione.
-

3. Necessità e proporzionalità del trattamento

Necessità

La PA necessita di un canale di comunicazione immediato e multilingua, anche per cittadini privi di identità digitale, SIM e applicazioni commerciali.

Proporzionalità

- Nessuna raccolta sistematica di dati personali.
- Nessuna profilazione.
- Nessun logging dei contenuti.
- I tecnici PA hanno piena autonomia (open source, server in-house).

Il trattamento risulta pienamente proporzionato e minimizzato (art. 5(1)(c) GDPR).

4. Valutazione dei rischi per gli interessati

4.1 Rischi identificati

1. **Intercettazione del traffico dati**
2. **Accesso non autorizzato alle sessioni attive**
3. **Furto di file trasferiti durante la chat**

4. **Malconfigurazione del server da parte della PA**

5. **Errore umano (inviare dati sensibili nel testo)**

4.2 Valutazione preliminare del rischio

- I rischi sono **temporanei**, poiché i dati non vengono conservati.
- L'esposizione massima coincide con la durata della singola sessione.

5. Misure di mitigazione implementate

Rischio	Misure Loquimini	Valutazione
Intercettazione	TLS completo, server PA	Adeguata
Accesso non autorizzato	Link hash random, sessioni monouso, cartelle effimere	Alta sicurezza
Fughe di dati	Nessuna conservazione, distruzione automatica	Rischio minimale
Configurazione errata	Virtualmin, formazione 10h, documentazione sorgenti	Mitigazione sostanziale
Errori utente	Sessioni anonime senza metadati, minimizzazione	Adeguata

6. Confronto con alternative esterne (WhatsApp, Telegram, WeChat, Google Translate)

6.1 Conservazione dei dati

Sistema	Conservazione dati	Luogo
Loquimini	Nessuna	On-premise PA
WhatsApp	Sì	Meta (USA)
Telegram	Variabile	Extra-UE
WeChat	Sì, massiva	Cina
Google Translate	Contenuto inviato ai server Google	Extra-UE

6.2 Conformità GDPR

Sistema	Conformità per uso istituzionale
Loquimini	Sì (progettato privacy-by-design, on-premise)
WhatsApp	No (uso istituzionale sconsigliato dal Garante)
Telegram	No (sede non UE, criptazione opzionale)
WeChat	No (pratiche invasive)
Google Translate	No (dati inviati a terzi extra-UE)

6.3 Dipendenza da terze parti

- **Loquimini**: 0% (server PA, sorgenti aperti).
- WhatsApp/Telegram/WeChat: 100%.

- Google: 100%.

6.4 Identificabilità utenti

Sistema	Richiede telefono?
Loquimini	No
WhatsApp	Sì
Telegram	Sì
WeChat	Sì
Google Translate	No, ma invio dati a terzi

6.5 Sintesi

Loquimini è l'unico sistema realmente compatibile con i requisiti GDPR e privacy-by-design per un uso PA, garantendo:

- totale autonomia tecnica,
 - zero conservazione,
 - anonimato,
 - open source,
 - multilingua integrato,
 - controllabilità del codice.
-

7. Valutazione finale e residuo del rischio

Dopo le misure implementate, il rischio residuo è **basso**.

Non sono presenti elementi che suggeriscano rischi elevati tali da richiedere la consultazione preventiva del Garante (art. 36 GDPR).

8. Conclusioni

Il sistema **Loquimini**, per architettura tecnica e modalità operative, soddisfa in modo esemplare i principi GDPR:

- privacy by design e by default (art. 25),
- minimizzazione dei dati (art. 5),
- sicurezza del trattamento (art. 32),
- trasparenza e controllabilità per la PA.

È particolarmente idoneo per:

- sportelli al cittadino,
- comunicazioni multilingua,

- contesti delicati che richiedono anonimato e non tracciabilità,
 - enti pubblici che non vogliono dipendere da servizi commerciali esteri.
-