MyBrokerage AI
Empowering Human in Real Estate

SICUREZZA & COMPLIANCE

Misure di sicurezza, infrastruttura e conformita' normativa

Versione **v1.0** | In vigore dal **05 gennaio 2026** | Pubblicazione pubblica — /legal/security
GogoVest S.r.l. | Via Salento 61, 00162 Roma (RM) | C.F. / P.IVA 14688251009 | privacy@mybrokerage.ai

Il presente documento descrive le misure tecniche, organizzative e normative adottate da GogoVest S.r.l. per garantire la sicurezza della Piattaforma MyBrokerage AI e la conformita' alle normative applicabili.

1. Infrastruttura e certificazioni

La Piattaforma e' ospitata su infrastrutture primarie in Italia presso fornitori certificati. Le certificazioni di seguito indicate sono quelle in vigore alla data di pubblicazione del presente documento, così come comunicate dal fornitore di infrastruttura. Il Fornitore non puo' essere ritenuto responsabile per eventuali variazioni successive delle certificazioni del proprio fornitore di infrastruttura, fermo restando l'impegno ad aggiornare la presente documentazione in caso di modifiche rilevanti.

- ISO/IEC 27001:2022 — Gestione della sicurezza delle informazioni
- ISO/IEC 27017:2015 — Sicurezza nel cloud computing
- ISO/IEC 27018:2014 — Protezione dei dati personali nel cloud pubblico
- ISO 22301:2019 — Business continuity management
- ISO 20000-1:2018 — IT service management
- ISO 9001:2015 — Gestione della qualita'
- ISO 14001:2015 — Gestione ambientale
- CISPE — Cloud Infrastructure Services Providers in Europe
- CSA STAR Level 1 — Cloud Security Alliance
- DNSH (Do No Significant Harm) compliance

2. Continuita' operativa e disaster recovery

Sistemi di business continuity e disaster recovery garantiscono la continuita' del servizio. In caso di indisponibilita' dell'infrastruttura primaria vengono attivate automaticamente infrastrutture di backup europee, conformi ai requisiti normativi.

3. Localizzazione e trasferimento dei dati

I dati sono localizzati prevalentemente nell'UE. I backup cifrati possono essere distribuiti su infrastrutture europee per garantire la resilienza. Eventuali trasferimenti extra UE avvengono nel rispetto delle garanzie GDPR (clausole contrattuali standard o decisioni di adeguatezza).

4. Sicurezza tecnica

4.1 Crittografia e accessi

- Dati in transito protetti da HTTPS/TLS
- Credenziali protette tramite hashing con salt
- Autenticazione a piu' fattori (2FA) per accessi privilegiati
- Controllo accessi basato su ruoli (RBAC)
- Limitazione degli accessi al minimo necessario

4.2 Isolamento e monitoraggio

- Architettura progettata per garantire la separazione dei dati tra Organizzazioni distinte
- Logging completo delle operazioni amministrative (audit trail)
- Monitoraggio continuo per accessi anomali e attivita' sospette
- Alert automatici per attivita' potenzialmente fraudolente

5. Flussi di trattamento dei dati

I dati provengono da: inserimento manuale degli utenti; portali immobiliari e canali autorizzati; sistemi automatici da mittenti autorizzati; API, webhook e automazioni configurate dal cliente; canali di comunicazione personali (es. WhatsApp Cloud API). Le integrazioni con sistemi esterni sono configurate dal cliente, che ne e' responsabile.

6. Minimizzazione e conservazione

La Piattaforma adotta sistemi automatici per limitare il trattamento ai dati necessari e filtrare comunicazioni non pertinenti. Le comunicazioni ricevute tramite sistemi di inoltro automatico (es. email forwarding) che non siano riconducibili alle finalita' del servizio vengono eliminate entro un periodo tecnico normalmente non superiore a ventotto (28) giorni dal ricevimento, senza archiviazione persistente e senza indicizzazione. L'accesso a tali comunicazioni da parte del personale tecnico e' consentito esclusivamente per finalita' di debug e supporto, e' tracciato tramite audit log e avviene adottando misure volte a limitare l'accesso al minimo necessario.

I dati sono conservati per la durata del rapporto contrattuale. Alla cessazione: export disponibile per un periodo indicativamente non superiore a 90 giorni; rimozione dai sistemi attivi entro i 60 giorni successivi; backup soggetti a rotazione tecnica ed eliminati comunque entro ventotto (28) giorni dalla cessazione; dati fiscali conservati per obbligo di legge.

7. Gestione degli incidenti

In caso di violazione: analisi interna immediata; notifica al cliente senza ingiustificato ritardo; adozione di misure di contenimento e rimedio. Il Fornitore mantiene documentazione interna degli incidenti rilevati.

8. Intelligenza artificiale

I dati non vengono utilizzati dal Fornitore per l'addestramento di modelli di intelligenza artificiale generici. Le funzionalita' AI sono attivate esclusivamente previa accettazione esplicita tramite procedura in-app.

9. Ruoli GDPR

- L'Organizzazione e l'Utente Individuale agiscono quali Titolari del trattamento per i rispettivi dati
- GogoVest S.r.l. agisce quale Responsabile del trattamento ai sensi dell'art. 28 GDPR

10. Documentazione e audit

Ulteriori dettagli tecnici sono disponibili su richiesta (due diligence, vendor qualification, audit interni). Il Fornitore supporta attivita' di verifica della conformita' previa definizione delle modalita'.

11. Contatti

- GogoVest S.r.l.
- Via Salento 61, 00162 Roma (RM)
- Email: privacy@mybrokerage.ai
- Web: www.mybrokerage.ai

GogoVest S.r.l.
Via Salento 61, 00162 Roma (RM) | C.F. / P.IVA 14688251009
privacy@mybrokerage.ai | www.mybrokerage.ai
Sicurezza & Compliance — Versione 1.0 — In vigore dal 05 gennaio 2026