

DICHIARAZIONE DI CONFORMITÀ

Conformità dell'Assistente AI ad AI Act e GDPR

Sito: creazionesitiweb.xyz

Versione 1.1 — 10 luglio 2026

1. Premessa e ambito

Il presente documento descrive il funzionamento dell'assistente conversazionale basato su intelligenza artificiale (di seguito "l'Assistente AI") integrato nel sito **creazionesitiweb.xyz** e ne attesta la conformità al **Regolamento (UE) 2024/1689** (di seguito "AI Act") e al **Regolamento (UE) 2016/679** (di seguito "GDPR"). Si tratta di una dichiarazione di conformità del deployer (utilizzatore) del sistema, non di una certificazione rilasciata da un ente terzo.

I dati identificativi del Titolare del trattamento e del deployer del sistema AI sono riportati nella sezione contatti pubblicata in homepage (<https://creazionesitiweb.xyz/#contatti>) e nella Privacy Policy (<https://creazionesitiweb.xyz/privacy-policy>), alle quali si rinvia integralmente.

2. Descrizione del sistema

- **Nome:** Assistente AI di Creazione Siti Web.
- **Finalità:** assistenza informativa pre-contrattuale e commerciale (illustrazione dei servizi, risposte alle FAQ, invito alla consulenza gratuita).
- **Modello sottostante:** Large Language Model generativo di Google (famiglia Gemini) accessibile tramite gateway Lovable AI. Il deployer non addestra né effettua fine-tuning del modello.
- **Interfaccia:** chat widget testuale, accessibile dal sito, con dichiarazione esplicita che l'utente sta interagendo con un sistema AI.
- **Uscite del sistema:** risposte testuali informative. L'Assistente AI **non produce decisioni automatizzate** con effetti giuridici o significativi sulle persone.

3. Classificazione ai sensi dell'AI Act

L'Assistente AI è un sistema AI ai sensi dell'art. 3(1) AI Act. La classificazione del rischio è la seguente:

- **Pratiche vietate (art. 5):** non applicabile. Il sistema non impiega tecniche subliminali, non effettua social scoring, non inferisce emozioni, non esegue categorizzazione biometrica.
- **Alto rischio (Allegato III):** non applicabile. Il sistema non è usato in ambiti quali biometria, infrastrutture critiche, istruzione, occupazione, servizi essenziali, forze dell'ordine, migrazione o giustizia.

- **Rischio limitato (art. 50): applicabile.** Trattandosi di sistema AI che interagisce direttamente con persone fisiche, si applicano gli obblighi di trasparenza previsti dall'art. 50 AI Act.

Il deployer non è provider ai sensi dell'art. 25 AI Act, in quanto non sviluppa il modello sottostante né lo commercializza con proprio marchio; utilizza un modello di uso generale (GPAI) fornito da terzi.

4. Misure di conformità all'AI Act

4.1 Trasparenza (art. 50)

- Nel widget di chat è indicato in modo chiaro “Assistente AI” e la prima risposta comunica esplicitamente all'utente che sta interagendo con un sistema di intelligenza artificiale.
- Le risposte generate sono di natura informativa e non sono presentate come consulenza professionale personalizzata.

4.2 Supervisione umana

- L'utente può in qualsiasi momento richiedere il contatto con un operatore umano tramite il pulsante dedicato e tramite la pagina Contatti.
- Nessuna decisione contrattuale, economica o giuridica viene assunta autonomamente dal sistema. Preventivi, offerte e condizioni sono sempre confermati da personale umano.

4.3 Robustezza e sicurezza

- Prompt di sistema vincolato ai servizi del deployer, con divieto esplicito di inventare dati, statistiche o prezzi fissi.
- Validazione lato server dei messaggi in ingresso: limiti su numero (max 20 messaggi per richiesta) e lunghezza (max 2.000 caratteri per messaggio) per prevenire abusi e prompt injection su larga scala.
- Gestione controllata degli errori del gateway AI (codici 402, 429, 500) con messaggi generici all'utente e log lato server.
- Chiave API del gateway custodita esclusivamente lato server (Edge Function), mai esposta al browser.

4.4 Alfabetizzazione AI (art. 4)

Il personale del deployer che progetta, integra e mantiene l'Assistente AI possiede un livello adeguato di alfabetizzazione all'intelligenza artificiale, conoscendo capacità, limiti e rischi del modello utilizzato.

4.5 Non applicabilità dell'obbligo di marcatura (art. 50, par. 4)

L'obbligo di marcatura dei contenuti sintetici previsto dall'art. 50, par. 4, AI Act **non trova applicazione** al presente sistema. L'Assistente AI produce esclusivamente **testo conversazionale** all'interno del widget di chat e **non genera né diffonde deep-fake, immagini, audio o video sintetici** suscettibili di essere confusi con contenuti autentici. Il contesto d'uso (widget etichettato “Assistente AI” e disclosure esplicita in prima risposta) rende la natura generata del testo immediatamente riconoscibile all'utente ai sensi dell'art. 50, par. 1.

5. Conformità al GDPR

5.1 Titolare del trattamento

I dati identificativi del Titolare del trattamento sono riportati nella Privacy Policy (<https://creazione siti web.xyz/privacy-policy>) e nella sezione contatti in homepage.

5.2 Tipologia di dati trattati

- Contenuto testuale dei messaggi digitati volontariamente dall'utente durante la conversazione.
- Ove l'utente scelga di richiedere la consulenza gratuita: nome, email, telefono e informazioni fornite (esigenza, tempistica, budget).
- Non vengono trattate categorie particolari di dati (art. 9 GDPR); si invita l'utente a non inserire dati sensibili nella chat.

5.3 Base giuridica e finalità

- **Assistenza pre-contrattuale (chat):** art. 6(1)(b) GDPR — esecuzione di misure precontrattuali su richiesta dell'interessato; in via residuale art. 6(1)(f) — legittimo interesse a fornire assistenza commerciale.
- **Contatto per consulenza:** art. 6(1)(b) GDPR ed eventuale consenso specifico per la conservazione del contatto ai sensi dell'art. 6(1)(a).

5.4 Assenza di decisioni automatizzate (art. 22 GDPR)

L'Assistente AI **non effettua profilazione** né adotta decisioni automatizzate che producano effetti giuridici o incidano in modo significativo sull'interessato.

5.5 Conservazione e sicurezza

- I messaggi della chat **non sono persistiti** nel database del deployer: transitano dal browser dell'utente all'Edge Function e da questa al gateway AI, senza salvataggio strutturato lato server.
- I dati inviati tramite il form di consulenza sono memorizzati nel database del deployer, protetti da Row Level Security (RLS) e accessibili solo al personale autorizzato con ruolo di amministratore.
- Trasmissione dati in HTTPS (TLS). Secret e chiavi API custoditi esclusivamente lato server.

5.6 Destinatari e subresponsabili

- **Lovable** (fornitore piattaforma di hosting e AI gateway): server nell'Unione Europea per l'hosting dell'applicazione.
- **Google LLC** (fornitore del modello Gemini attraverso il gateway): il transito dei prompt può comportare trasferimento extra-UE verso gli Stati Uniti, coperto dalle Standard Contractual Clauses approvate dalla Commissione Europea e dal DPF (Data Privacy Framework) UE-USA.

5.7 Diritti dell'interessato

L'interessato può esercitare in qualsiasi momento i diritti di cui agli artt. 15-22 GDPR (accesso, rettifica, cancellazione, limitazione, portabilità, opposizione, revoca del consenso), secondo le modalità indicate nella Privacy Policy. È inoltre riconosciuto il diritto di proporre reclamo al Garante

per la Protezione dei Dati Personali (www.garanteprivacy.it).

5.8 Valutazione d'impatto (DPIA)

Il trattamento operato tramite l'Assistente AI **non rientra tra i casi di DPIA obbligatoria** ai sensi dell'art. 35 GDPR e delle Linee guida WP248 del WP29 / EDPB: non comporta monitoraggio sistematico su larga scala, non tratta categorie particolari di dati, non produce decisioni automatizzate con effetti significativi. È stata comunque effettuata una valutazione preliminare del rischio, con esito basso.

6. Misure di sicurezza tecniche e organizzative

- Trasmissione dati esclusivamente in HTTPS (TLS 1.2+).
- Validazione e sanitizzazione degli input lato server.
- Rate limiting e limiti dimensionali sulle richieste al gateway AI.
- Row Level Security (RLS) su tutte le tabelle contenenti dati personali; accesso all'area amministrativa gated tramite autenticazione e ruolo.
- Secret e chiavi API gestiti come environment variables server-side, mai esposti al client.
- Aggiornamenti periodici delle dipendenze e review di sicurezza automatica del codice.

7. Governance e revisione

Il presente documento è riesaminato almeno una volta l'anno e ogni volta che intervenga una modifica sostanziale del sistema (cambio di modello, nuove finalità di trattamento, nuove funzionalità), o comunque a seguito di aggiornamenti significativi della normativa applicabile.

8. Riferimenti normativi

- Regolamento (UE) 2024/1689 — Artificial Intelligence Act
- Regolamento (UE) 2016/679 — General Data Protection Regulation (GDPR)
- D.Lgs. 196/2003 come modificato dal D.Lgs. 101/2018
- Direttiva 2002/58/CE (ePrivacy)
- Linee guida EDPB in materia di trasparenza, base giuridica e trasferimenti internazionali

9. Registro delle versioni

Versione	Data	Modifiche
1.0	10 luglio 2026	Prima emissione
1.1	10 luglio 2026	Riformulazione § 4.5 come esplicita non applicabilità art. 50(4); allineamento Privacy Policy sui subresponsabili extra-UE (Lovable / Google Gemini via gateway AI)

10. Contatti

Per informazioni sul sistema AI descritto, sui trattamenti di dati personali ivi effettuati o per esercitare i diritti riconosciuti dal GDPR, si rinvia alla sezione contatti in homepage (<https://creazionesitiweb.xyz/#contatti>) e alla Privacy Policy (<https://creazionesitiweb.xyz/privacy-policy>), che contengono i dati identificativi aggiornati del Titolare del trattamento.