ALLEGATO A: ACCORDO SUL TRATTAMENTO DEI DATI (DPA)

Ai sensi dell'Art. 28 del Regolamento (UE) 2016/679 ("GDPR")

Il presente Accordo sul Trattamento dei Dati ("DPA") costituisce parte integrante e sostanziale dei Termini e Condizioni di Servizio di **ThermoThunder**.

Tra:

1. **L'Utente** (di seguito "**Titolare**" o "Controller"), che utilizza il Servizio per finalità professionali;
2. **Ruben Ganzerli** / **ThermoThunder** (di seguito "**Responsabile**" o "Processor"), fornitore del Servizio.

(Congiuntamente le "Parti").

1. Oggetto e Natura del Trattamento

Il Responsabile si impegna a trattare i Dati Personali di titolarità dell'Utente esclusivamente per l'erogazione dei servizi previsti dai Termini e Condizioni (servizi SaaS di analisi energetica, finanziaria e gestione progetti), e secondo le istruzioni documentate del Titolare. L'utilizzo stesso della Piattaforma e delle sue funzionalità da parte dell'Utente costituisce istruzione documentata al trattamento.

2. Tipologia di Dati e Categorie di Interessati

- **Categorie di Interessati:** Clienti finali dell'Utente (es. proprietari di immobili, committenti), dipendenti o collaboratori dell'Utente.
- **Tipologie di Dati:** Dati anagrafici (Nome, Cognome), dati di contatto, indirizzi degli immobili, dati relativi ai consumi energetici, caratteristiche tecniche degli edifici e qualsiasi altro dato personale inserito dall'Utente nella Piattaforma.

3. Obblighi del Responsabile (ThermoThunder)

Il Responsabile garantisce di:

1. **Istruzioni:** Trattare i dati personali esclusivamente su istruzione documentata del Titolare, salvo che lo richieda il diritto dell'Unione o nazionale cui è soggetto il Responsabile.
2. **Riservatezza:** Garantire che le persone autorizzate al trattamento (dipendenti, collaboratori) si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza.
3. **Sicurezza (Art. 32 GDPR):** Adottare tutte le misure tecniche e organizzative adeguate a garantire un livello di sicurezza commisurato al rischio (es. crittografia, pseudonimizzazione, resilienza dei sistemi, procedure di disaster recovery).
4. **Assistenza:** Assistere il Titolare, per quanto possibile e mediante misure tecniche adeguate, nel soddisfare le richieste degli interessati (es. diritto di accesso, cancellazione) e negli obblighi di sicurezza, notifica violazioni e valutazione d'impatto (DPIA).

5. **Cancellazione:** Al termine della fornitura del servizio, cancellare o restituire tutti i dati personali al Titolare, salvo che la legge non preveda la conservazione.

4. Sub-Responsabili (Sub-processors)

4.1. Il Titolare autorizza fin d'ora il Responsabile a ricorrere ad altri responsabili del trattamento ("Sub-responsabili") per l'erogazione del servizio (es. Cloud Provider come Google Cloud, Vercel, Supabase; Payment Processor come Stripe).
4.2. Il Responsabile impone ai Sub-responsabili, mediante contratto scritto, gli stessi obblighi di protezione dei dati contenuti nel presente accordo.
4.3. **Modifiche ai Sub-responsabili:** Il Responsabile informerà il Titolare di eventuali modifiche riguardanti l'aggiunta o la sostituzione di altri responsabili del trattamento con un preavviso di almeno **15 (quindici) giorni** (tramite e-mail, notifica in piattaforma o aggiornamento della lista pubblica), dando così al Titolare la possibilità di opporsi a tali modifiche per giustificati motivi legati alla protezione dei dati. In caso di opposizione non risolvibile, il Titolare avrà facoltà di recedere dal servizio.

5. Trasferimenti Extra-UE

Qualora i dati vengano trasferiti fuori dallo Spazio Economico Europeo (SEE), il Responsabile garantisce che tale trasferimento avverrà sulla base di garanzie appropriate, quali Decisioni di Adeguatezza (es. Data Privacy Framework UE-USA) o la sottoscrizione di Clausole Contrattuali Standard (SCC) approvate dalla Commissione Europea.

6. Violazione dei Dati (Data Breach)

Il Responsabile notificherà al Titolare qualsiasi violazione dei dati personali senza ingiustificato ritardo dopo esserne venuto a conoscenza, fornendo le informazioni necessarie (natura della violazione, categorie di dati coinvolte, misure adottate) affinché il Titolare possa adempiere ai propri obblighi di notifica all'Autorità di Controllo.

7. Audit e Ispezioni

Il Responsabile metterà a disposizione del Titolare tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui al presente articolo. Considerata la natura SaaS del servizio e l'utilizzo di infrastrutture Cloud condivise, le Parti convengono che le attività di audit fisico saranno limitate a casi eccezionali e potranno essere soddisfatte mediante la fornitura di certificazioni di sicurezza di terze parti (es. ISO 27001, SOC 2) o report di audit dei fornitori di infrastruttura.

8. Clausola di Prevalenza

In caso di conflitto o discrepanza tra le disposizioni del presente DPA e le disposizioni dei Termini e Condizioni di Servizio (o qualsiasi altro accordo tra le parti), le clausole del presente DPA prevarranno limitatamente a quanto attiene al trattamento e alla protezione dei dati personali.