

FlexOS: Technical & Security FAQ for Pilot Partners

1. Where is customer and meter data hosted, and is it secure?

Answer: All core cloud infrastructure and database instances are hosted within secure UK/EU cloud regions (AWS/GCP compliant architectures), ensuring full alignment with UK GDPR. Data in transit is encrypted via TLS 1.3, and data at rest uses AES-256 encryption.

2. How does FlexOS access UK smart meter (DCC) data without a supplier license?

Answer: FlexOS does not act as a licensed energy supplier. Instead, we natively bridge consumption feeds through accredited Phase 1 UK smart meter infrastructure partners (such as Hildebrand Glow), keyed directly to the property's Meter Point Administration Number (MPAN). To maintain a zero-friction customer experience, the installer simply secures standard data-access consent as part of their standard installation terms. This allows half-hourly telemetry ingestion without building a bespoke integration project for every energy supplier, and without requiring the homeowner to create a separate software account.

3. What happens to device control if a customer loses broadband connection?

Answer: FlexOS utilizes a local fallback architecture. The cloud optimization engine calculates and pushes day-ahead and interval dispatch schedules down to the edge hardware (Tuya, SmartThings, Matter integration layer). If a residential broadband drop occurs, the device executes its last-known local schedule uninterrupted, ensuring grid instructions are met even during network outages.

4. How are API credentials handled for inverter brands like SolarEdge and GivEnergy?

Answer: FlexOS uses a modular adapter pattern. During the brief commissioning wizard, your field technicians provide secure, scoped API read/write tokens generated via the respective manufacturer monitoring portals. FlexOS securely stores these tokens within encrypted environment vaults, using them strictly for telemetry reading and authorized load-shifting dispatch commands. The homeowner is never required to generate, manage, or provide API keys.

5. Is FlexOS ready for the May 2027 MHHS mandate?

Answer: Yes. FlexOS automatically reconciles half-hourly consumption and dispatch records against the DCC data pipeline. Every control action is timestamped and written to an immutable audit ledger, delivering settlement-ready records that satisfy both supplier and network operator compliance requirements ahead of the May 2027 Market-wide Half-Hourly Settlement deadline.