Host Privacy Standards — Furnished Rental Group (FRG)

This Host Privacy Standards Policy ("Policy") applies to all **Hosts** ("you," "your") providing accommodation or related services via the **Furnished Rental Group Platform** ("FRG Platform").

When processing Guest Personal Data, you agree to comply with:

- **Applicable privacy and data protection laws**, including GDPR (EEA), UK Data Protection Act, CCPA (California), LGPD (Brazil), PIPL (China), and other local regulations;
- **FRG Terms of Service**, **Payment Terms**, and **Privacy Policy**; and
- This **Host Privacy Standards Policy**.

---

1. Host Responsibilities for Guest Personal Data

1.1 Permitted Use of Guest Data

You may only process Guest Personal Data for:

- Managing reservations,
- Providing the Host Services (check-in, check-out, communication),
- Complying with legal or regulatory obligations,
- Coordinating services with authorized providers (e.g., cleaning, property management).

Any use beyond these purposes, such as marketing or profiling, is **strictly prohibited** unless required by law or explicitly authorized by FRG and the Guest.

1.2 Data Minimization & Retention

- Collect only the **minimum personal data necessary** to fulfill reservation obligations.

- Retain data **only for the period legally required** or reasonably necessary for service delivery and dispute resolution.

1.3 Prohibited Activities

Hosts **must not**:

- Encourage Guests to create accounts or interact with unauthorized third-party platforms before, during, or after reservations.
- Sell, lease, or share Guest Personal Data with third parties for advertising or unrelated purposes.
- Request unnecessary sensitive personal data unless legally required (e.g., identity verification for local guest registries).

---

2. Cross-Border Data Transfers

Where Guest Personal Data is transferred across borders, including from the **EEA, Switzerland, or UK** to third countries:

- Transfers must comply with **GDPR Chapter V** requirements.
- Where no **adequacy decision** exists under GDPR Article 45, the **EU Standard Contractual Clauses (SCCs)** for **Controller-to-Controller Transfers (Module 1)** under **Decision (EU) 2021/914** apply automatically.

2.1 Standard Contractual Clauses (SCCs)

For transfers subject to the SCCs:

- **Clause 7 (Docking Clause)**: Not applicable.
- **Clause 11 (Optional Redress Mechanism)**: Not applicable.
- **Clause 17 (Governing Law)**: Irish law governs the SCCs.

- **Clause 18 (Jurisdiction)**: Irish courts have exclusive jurisdiction.

2.2 SCC Annex Completion

- **Data Importer**: The Host receiving Guest Personal Data.
- **Data Exporter**:
    - **Japan**: FRG Global Services Limited.
    - **Brazil**: FRG Plataforma Digital Ltda (effective April 1, 2022).
    - **All other regions**: FRG Ireland UC.

Annex I.B — Data Details

- **Data Subjects**: Guests booking on the FRG Platform.
- **Purpose**: Delivery of Host Services and reservation management.
- **Categories of Data**:
    - Guest profile details, full name, contact information (phone, email), reservation history, messages exchanged, and additional travel coordination details.
- **Recipients**:
    - Authorized service providers selected by the Host for operational purposes.
- **Sensitive Data**: None transferred unless required by law.
- **Frequency**: As determined by reservation activity.
- **Retention**: Data retained only as long as necessary for service delivery and compliance.

Annex I.C — Supervisory Authority

- **Lead Supervisory Authority**: Irish Data Protection Commission.

Annex II — Security Measures

Hosts must implement **technical and organizational security measures** in line with **GDPR Article 32**, including:

- **Encryption** and **pseudonymization** of personal data,
- Ensuring **confidentiality, integrity, availability**, and resilience of systems,
- **Disaster recovery and backup** capabilities,
- **Regular testing** of security measures for effectiveness.

---

3. Data Security Requirements

Hosts must ensure:

- Secure access controls for systems storing Guest data,
- Encryption for data in transit (e.g., TLS) and at rest where feasible,
- Timely reporting of any **data breaches** to FRG and relevant authorities per **GDPR Article 33** and applicable local laws.

---

4. Guest Rights & Compliance

Hosts must support FRG in responding to Guest rights requests under applicable laws, including:

- **Access**, **Rectification**, **Erasure** (Right to be Forgotten),
- **Restriction of Processing**, **Data Portability**, and **Objection** rights,
- Withdrawal of consent where applicable.

---

5. Regional Compliance Obligations

5.1 EEA & United Kingdom

- GDPR and UK Data Protection Act compliance required.
- Data Protection Impact Assessments (DPIAs) for high-risk processing activities.

5.2 United States (California)

- **CCPA** obligations for California residents:
    - Right to opt-out of data sharing,
    - Right to deletion, access, and non-discrimination.

5.3 Brazil

- **LGPD** obligations for lawful processing, data subject rights, and data protection officer (DPO) responsibilities.

5.4 China

- **PIPL** obligations for cross-border transfers, localization requirements, and consent-based processing.

5.5 Japan

- **APPI** obligations for data handling, security measures, and international transfers.

---

6. Enforcement & Penalties

Violations of this Policy may result in:

- **Suspension or termination** of Host accounts,
- **Withholding of payouts**,
- **Reporting to authorities** where legally required,
- **Civil or criminal liability** under applicable laws.

7. Dispute Resolution

Disputes arising under this Policy follow:

- **FRG Terms of Service** arbitration provisions for U.S. users,
- **Local dispute resolution mechanisms** for EEA, UK, Brazil, China, and other jurisdictions as applicable.

---

8. Modifications

FRG may update this Policy to reflect:

- Changes in **data protection laws**,
- **Platform security enhancements**,
- Updated **regulatory guidance** from supervisory authorities.

Material changes will be communicated with at least **30 days' notice** before enforcement.

---

9. Effective Date

This Policy is effective as of **September 3, 2025**, unless otherwise required by local law.

This **Host Privacy Standards — FRG** policy now provides a **comprehensive global framework** for:

- **Host responsibilities**,
- **Cross-border transfers**,
- **Security measures**,

- **Data retention**, and
- **Regional legal compliance** under GDPR, CCPA, LGPD, PIPL, and other frameworks.