SOP-07 — GDPR Day-to-Day Data Handling

Trigger: Any processing of personal data of EEA, Swiss or UK residents. **Owner:** Compliance Officer (DPO role).

1. Lawful basis at point of capture

When building a new form, integration or workflow, the Compliance Officer signs off on the lawful basis before launch. Default mapping is in docs/compliance/07 § 2.

2. Data Subject Access Requests (DSARs)

1. Any request received at any address (charter@, privacy@, social, phone) is forwarded to privacy@thelimitlesssky.com within 1 business day.
2. Compliance verifies the requester's identity (without collecting more than necessary).
3. Compliance compiles the response across CRM, mailbox, support tool, booking files and finance.
4. Response within 30 days of request (extendable by 60 days for complex requests with notice).
5. Exercise of rights: access, rectification, erasure, restriction, portability, objection, withdraw consent, lodge complaint with a SA.

3. International transfers

Default: EU-US Data Privacy Framework certification. Where a processor is not DPF-certified, Compliance executes SCCs (Modules 1/2) and runs a TIA before go-live.

4. Processor onboarding

Every new processor signs the GDPR Art. 28 / UK DPA / FADP addendum, including SCCs where needed. Vendor list maintained by Compliance.

5. Breach handling

- Internal alert within 24 hours of detection.
- Compliance assesses Art. 33 / Art. 34 triggers.
- Notification to the lead SA within 72 hours where Art. 33 triggers.
- Notification to data subjects where Art. 34 triggers.
- Breach register entry (cause, scope, mitigation, notification status). Retained 5 years.

6. EU representative

The appointed Art. 27 representative is named in the Privacy Notice. Compliance forwards any contact from the representative within 1 business day.