SMEATON

Data Retention Policy

For Smeaton staff and contractors (internal use only)

This policy governs how personnel within Smeaton (including founders, developers such as contracted app developers, and any future employees or contractors) may access, use, and retain personal data processed through the Smeaton platform. It is an internal document, not shared with customers, though a summary of its existence may be referenced in the Privacy Policy.

1. Purpose

To ensure Smeaton only allows internal access to personal data (particularly Crew Data) where necessary, to document who can see what internally, and to set retention and deletion rules so that Smeaton can demonstrate compliance if audited by a customer, an insurer, or a regulator.

2. Internal roles and access levels

Role	Can access	Cannot access
Founder(s) / director(s)	Full platform data, for legitimate business administration, support, and compliance purposes only	N/A — access should still be logged and used only when necessary
App developer(s)	Data reasonably necessary for building, testing, and fixing the platform, ideally via anonymised or test data wherever possible	Should not routinely browse live customer/crew data outside of debugging a specific reported issue
Future customer support staff	Data needed to resolve the specific support ticket raised	Broader account/vessel data unrelated to the ticket

3. Principles

- Least privilege: internal access mirrors the external principle in the Data Sharing Policy — individual crew data is accessed internally only where there is a genuine operational reason (e.g. investigating a reported bug affecting a specific scan).
- Logging: access to identifiable Crew Data by internal personnel should be logged (who, when, what record, why) once the platform supports this — flag as a build requirement for Tom.
- Test/development data: wherever possible, development and QA should use synthetic or anonymised data rather than live customer data.
- Device and account security: any device or account with access to production data must use strong authentication (and multi-factor authentication once available).

4. Retention and deletion

- Live patrol/round/tag data: retained for 36 months then deleted or anonymised.
- Backups: backup copies are purged on a rolling basis no later than 12 months after the corresponding live data is deleted.
- Account data for churned customers: retained for 36 months after contract end to support any final reporting or dispute, then deleted.
- Documents containing personal data should not be stored in Google Drive (e.g. exports, reports).

5. Breach response

Any suspected personal data breach (unauthorised access, loss, or disclosure of Crew Data) must be escalated immediately to josh@smeatondata.com or tom@smeatondata.com. Smeaton must assess whether affected Customers need to be notified without undue delay under the DPA, and whether the breach is reportable to the ICO within 72 hours of Smeaton becoming aware of it.

6. Review

This policy should be reviewed whenever the technical architecture changes materially (e.g. new sub-processors, new roles, new features such as biometric login), and at least annually.