SMEATON

Privacy Policy

For the Smeaton patrol verification platform

Last updated: 18/09/2026. This policy explains how Bolt Tail Technologies operating the Smeaton application ("we", "us", "Smeaton") collects, uses, and protects personal data through the Smeaton application and NFC patrol verification system, in accordance with the UK GDPR, the EU GDPR (where applicable to vessels or data subjects within scope), and the Data Protection Act 2018.

1. Who we are

Smeaton is a security patrol verification service used on board superyachts and at marine facilities. Smeaton is provided by Bolt Tail Technologies Ltd, UK Company number 17174214, of 6 Sunnyside, South Milton, Devon, TQ7 3JW ("Smeaton", "we"). For most vessels, the yacht owner or the management company that contracts with us is the data controller for crew personal data, and Smeaton acts as a data processor on their behalf under a separate Data Processing Agreement. Where Smeaton determines the purposes of processing (for example, aggregate product analytics), Smeaton acts as controller for that specific processing.

2. What data we collect

Smeaton collects the following categories of data through the app and NFC tag network:

- Patrol event data: NFC tag ID scanned, timestamp, and the identity of the crew member or guard who performed the scan.
- Round data: which checkpoints were completed, in what order, and whether a round was completed within its expected time window.
- Device and location data: the vessel or site location associated with each tag, and, where enabled, device-level metadata needed to verify a scan was performed on site.
- Tag condition reports: reports of broken, missing, or tampered tags, and the time taken to resolve them.
- Account data: name, email address, phone number, role (e.g. Admin, Crew, Officer), and login credentials for anyone with access to the platform.
- Derived scores: the 'Smeaton Index', 'SI' and related sub-scores (e.g. round adherence, tag-fault resolution), which are calculated from the data above.

3. Why we process this data, and our lawful basis

We process personal data for the following purposes:

- To verify that security patrols were physically carried out as scheduled — necessary for the performance of the contract between Smeaton and the customer (Art. 6(1)(b) GDPR), and for the legitimate interests of the vessel operator in maintaining a safe, secure vessel (Art. 6(1)(f)).

- To calculate performance scores used by the captain to manage crew and by owners to assess overall security performance at an aggregate level — legitimate interests (Art. 6(1)(f)), balanced against crew members' expectations of privacy (see Section 5).
- To share aggregated, de-identified performance data with owners, brokers, marinas, or insurers where the customer has instructed us to do so — legitimate interests of the controller, subject to the data-minimisation approach described in Section 5.
- To maintain and improve the Smeaton platform, including security and fault diagnosis — legitimate interests (Art. 6(1)(f)).

We do not currently rely on consent as our primary lawful basis for patrol verification data, because crew members are not in a position to freely withhold consent from an employer-mandated system. Where any future use of data would require consent (for example, an optional feature), we will ask for it separately and specifically.

3A. Determining international transfer requirements

For the purposes of assessing whether an international data transfer safeguard (such as a UK International Data Transfer Agreement) is required, Smeaton will rely on the registered business address of the Customer's contracting entity (the owner company, management company, broker, or insurer entering into these Terms), not the flag state or port of registration of any vessel. Where the Customer's registered address is outside the UK and EEA and is not covered by a UK adequacy decision, Smeaton will require an appropriate transfer mechanism to be executed before granting full account access, in accordance with Clause 7 of the Data Processing Agreement.

4. Special category data

Smeaton does not intentionally collect special category data (e.g. health, biometric-for-identification, or similar sensitive data) as defined by Article 9 GDPR. NFC scans identify a tag and a logged-in user account; they do not use biometric identification. If this changes — for example, if facial recognition or biometric login is added — this policy and the underlying lawful basis will be updated.

5. Who can see what — our data minimisation approach

A core design principle of Smeaton is that individually identifiable crew performance data is only visible to those with an operational need to see it, and that performance scoring specifically is visible only to those responsible for managing the crew:

- All crew members can see which named individual completed each patrol round, including timing and tag condition reports, as this reflects the shared on-board record of duties performed. Crew members do not see performance scores — their own or anyone else's — calculated from this data.
- Captains and designated on-board security officers can additionally see individual performance scores and sub-scores calculated from this data, in order to manage day-to-day performance and address any shortfalls directly.

- Yacht owners, charter companies, brokers, marinas, and insurers receive only aggregated or anonymised data — for example, an overall Smeaton Index score for the vessel or a rolling round-adherence percentage — and do not see which named individual performed a given patrol or scan, unless disclosure of an individual's data is separately required (for example, in connection with a specific security incident, insurance claim investigation, or legal obligation, and then only to the minimum extent necessary).

This boundary is set out in more detail in our Data Sharing and Third-Party Disclosure Policy, which forms part of our contractual terms with customers.

6. How long we keep data

We retain patrol event data, round data, and tag condition data for 36 months from the date of collection, after which it is deleted or fully anonymised, unless a longer period is required to comply with a legal obligation, resolve a dispute, or support an active insurance or incident investigation. Account data is retained for as long as the account is active, plus 36 months after closure.

7. Who we share data with

We share data with:

- The vessel's owner, management company, or their nominated representatives, in aggregated/anonymised form as described in Section 5.
- Brokers, marinas, or insurers only where the customer (as data controller) has instructed us to provide aggregated reporting to that party, and only to the extent instructed.
- Sub-processors who help us run the platform: Amazon Web Services (AWS) for cloud hosting, and Google Drive for internal administrative document storage — Google Drive is not used to store customer or crew personal data. See our Sub-processors page for the current list, updated in accordance with our Data Processing Agreement. https://smeatondata.com/subprocessors.php
- Regulators, law enforcement, or other parties where required by law.

We do not sell personal data, and we do not share individually identifiable crew data with owners, brokers, or insurers as a matter of course.

8. International transfers

Smeaton hosts all platform data in the United Kingdom. Where personal data originates from a vessel, owner, or management company based in the EEA, transfers to our UK servers are permitted without additional safeguards under the UK-EU adequacy arrangement. Where a customer, broker, or insurer is based outside the UK and EEA in a jurisdiction not covered by an adequacy decision, we will put an appropriate transfer mechanism in place (such as the UK International Data Transfer Agreement) before providing them with access to personal data. Our insurance partners, as UK-based Lloyd's syndicates, are not subject to international transfer restrictions under this policy.

9. Data subject rights

Crew members and other data subjects have the right to access, correct, delete, restrict, or port their personal data, and to object to processing based on legitimate interests, subject to applicable exemptions. Requests should be directed to hello@smeatondata.com. Because Smeaton typically acts as a processor for crew data, some requests may need to be directed to, or coordinated with, the vessel owner or management company as controller.

10. Security

We apply technical and organisational measures appropriate to the sensitivity of the data, including role-based access controls consistent with Section 5, encryption in transit and at rest, and regular review of who has access to what.

11. Contact and complaints

Questions or complaints about this policy can be sent to hello@smeatondata.com. UK-based data subjects also have the right to complain to the Information Commissioner's Office (ico.org.uk).

12. Business transfers

If Smeaton, or substantially all of its assets, is involved in a merger, acquisition, investment, or sale of business, personal data may be transferred to the acquiring or surviving entity as part of that transaction. Where this occurs, we will ensure the receiving entity is bound to protect personal data to a standard consistent with this policy, and we will provide notice to affected customers before any personal data is transferred and becomes subject to a materially different privacy policy. This clause does not affect the underlying data protection obligations owed to crew members and other data subjects, which continue regardless of any change in corporate ownership.

13. How and when this policy is provided to you

If you are a crew member, guard, or other end user of the Smeaton app, this policy (or a summary of it, linking through to the full text) is shown to you on your first login to the app. Tapping "I understand" or continuing past that notice records that you have been given this information, as required by transparency obligations under GDPR — it does not create a contract between you and Smeaton, since your employer or the vessel's management company is the party that contracts with Smeaton on your behalf. If you have questions about how your data is used, you can raise them with your captain, your employer, or directly with Smeaton using the contact details above.