SMEATON

Data Agreement

Between Smeaton (Processor) and the Customer (Controller)

This Data Processing Agreement ("DPA") is entered into between Bolt Tail Technologies Ltd, UK company number 17174214 ("Processor", "Smeaton"), operating the Smeaton platform, and the customer entity that accepts the Smeaton Terms of Service through the Smeaton platform, as identified by the legal name, registered address and (where applicable) company number recorded against its account at the time of acceptance ("Controller", "Customer"). This DPA forms part of the Smeaton Terms of Service (the "Principal Agreement") and takes effect on the Effective Date as defined in the Principal Agreement. It applies wherever Smeaton processes personal data on the Customer's behalf in connection with the Smeaton platform.

1. Definitions

Terms such as "personal data", "processing", "controller", "processor", "data subject", and "personal data breach" have the meanings given in the UK GDPR / EU GDPR as applicable. "Crew Data" means personal data relating to identifiable crew members, guards, or other vessel personnel processed via the Smeaton platform.

2. Roles of the parties

The Customer is the controller of Crew Data. Smeaton is the processor and will process Crew Data only on the Customer's documented instructions, as set out in the Principal Agreement, this DPA, and any subsequent written instructions, except where otherwise required by law (in which case Smeaton will inform the Customer of that legal requirement, unless prohibited from doing so).

3. Subject matter, duration, nature and purpose of processing

Subject matter	Provision of NFC-based security patrol verification and performance scoring via the Smeaton platform.
Duration	For the term of the Principal Agreement, plus any period required for data return/deletion under Clause 4.
Nature of processing	Collection, storage, aggregation, scoring, and reporting of patrol event data.
Purpose	To verify patrol completion, generate performance scores, and provide reporting to the Customer and its authorised recipients.
Categories of data subjects	Crew members, security guards, and other on-board or on-site personnel using the Smeaton app.
Categories of personal data	Name, email address, phone number, role, NFC scan timestamps and locations, round completion data, tag condition reports, account login data, and derived performance scores.

4. Smeaton's obligations

- Process Crew Data only on the Customer's documented instructions, including with regard to onward disclosure to owners, brokers, marinas, or insurers.
- Ensure persons authorised to process Crew Data are subject to confidentiality obligations.
- Implement appropriate technical and organisational security measures, including the role-based access restriction described in Clause 5.
- Not engage a sub-processor without the Customer's prior general or specific written authorisation, and ensure any sub-processor is bound by data protection terms no less protective than this DPA.
- Assist the Customer, insofar as reasonably possible, in responding to data subject access requests and in meeting its obligations regarding security, breach notification, and data protection impact assessments.
- Notify the Customer without undue delay, and in any event within 48 hours of becoming aware, of any personal data breach affecting Crew Data.
- At the Customer's choice, delete or return all Crew Data at the end of the provision of services, and delete existing copies unless retention is required by law.
- Make available to the Customer all information reasonably necessary to demonstrate compliance with this DPA, and allow for audits, including inspections, conducted by the Customer or an auditor mandated by the Customer, on reasonable notice.

5. Access restriction — individual crew data

Smeaton will configure the platform so that: (a) all crew members can see which named individual completed each patrol round, including timing and tag condition reports, as a shared operational record; (b) individually identifiable performance scores calculated from Crew Data are accessible only to the vessel's captain and designated on-board security managers nominated by the Customer; and (c) owners, brokers, marinas, and insurers granted access to the platform or to reporting outputs will, by default, receive only aggregated or anonymised data (e.g. vessel-level 'Smeaton Index', 'SI' scores), unless the Customer provides specific written instructions to disclose named individual data for a defined purpose (for example, an incident investigation).

6. Sub-processors

The Customer authorises Smeaton's use of the sub-processors listed at https://smeatondata.com/subprocessors.php as updated from time to time in accordance with this Clause. As at the date of this DPA, those sub-processors are Amazon Web Services (AWS), for cloud hosting and infrastructure, and Google Drive, for internal business document storage. Google Drive is used solely for internal administrative purposes and does not process Crew Data. Smeaton will give the Customer at least 30 days' notice of any intended addition or change to this list, during which the Customer may object on reasonable data protection grounds. Smeaton will ensure any sub-processor is bound by data protection terms no less protective than this DPA.

7. International transfers

Where Crew Data is transferred outside the UK or EEA, Smeaton will ensure an appropriate transfer mechanism is in place (such as the UK International Data Transfer Agreement or EU Standard Contractual Clauses) before the transfer occurs. For the purposes of this Clause, the relevant jurisdiction is the Customer's registered business address, not the flag state of any vessel.

8. Liability and term

This DPA takes effect on the Effective Date and continues for as long as Smeaton processes Crew Data on the Customer's behalf. Liability between the parties is governed by the liability provisions of the Principal Agreement.

9. Governing law

This DPA is governed by the laws of England and Wales, consistent with the governing law of the Principal Agreement. The parties submit to the exclusive jurisdiction of the courts of England and Wales in relation to any dispute arising out of or in connection with this DPA.