

Privacy Boundaries

Short product-specific trust overview for website visitors, pilots and first discussions.

Aware Mate supports active watchkeeping. It is not a surveillance product.

These boundaries describe the default privacy and use position for pilots and standard deployments. Customer-specific settings are agreed in the pilot scope, data-processing terms and operator SOP.

1. Core default boundaries

On-board processing by default	Advisory only	No identity recognition
No emotion recognition	No raw video ashore by default	No person-level profiling or scoring
No worker evaluation	No automated discipline	Human review required

2. What Aware Mate is for - and not for

Aware Mate can - Prompt locally when sustained watchkeeping patterns need attention. - Generate derived metadata and aggregated review outputs. - Support procedure, workload, training and pilot close-out review by authorised humans.	Aware Mate is not for - Live CCTV or remote bridge surveillance. - Identifying, ranking or scoring individual officers. - Emotion, stress, intent or personality inference. - Automated HR, discipline, blame or fitness-for-duty decisions. - Navigation control or ECDIS/radar/autopilot control.
---	--

3. Default shore review

Standard shore review may include - Period-level alert trends and severity mix. - Valid monitoring time and pilot KPI summary. - Alert load per monitored hour. - Aggregated long-absence flags, if enabled. - Context-weighted review, if agreed and available.	Standard shore review does not include - Continuous raw video feed or raw video ashore by default. - Officer identity, face identity or biometric profiles. - Exact event timestamps in basic aggregated review. - Automated conclusions about fault, intent or performance.
---	--

4. No profiling / no worker evaluation

Aware Mate is not for individual alert histories, personnel files, worker ranking, productivity scoring, appraisal, rostering, pay, promotion, discipline, dismissal, fitness-for-duty or medical decisions. Employer-facing review should remain aggregate-first. Any documented incident-review exception requires written scope, lawful basis, access control, retention and audit logging.

5. Indirect identification is treated as a real risk

Watch schedules can identify people indirectly.

- Reports are designed to avoid person-level inference where possible. - Time-of-day charts are avoided by default where fixed watches can reveal roles or individuals. - Small-crew deployments may require additional aggregation, masking or access controls. - Deeper review or forensic buffers require explicit scope, access control, purpose limitation and retention rules.

6. Pilot governance commitments

Scope before install Vessel, bridge area, monitoring window, outputs, KPIs and responsibilities are agreed before installation.	Crew briefing first Crew are told what the system does, what shore does not see, and how mute, pause or override works.	Silent calibration Calibration precedes active use to reduce nuisance and validate the setup.
Controlled access Access is role-based. Remote support or additional export requires approval.	Retention rules Retention, deletion and exceptional review processes are agreed in writing.	Close-out review Findings are framed around procedures, workload and system fit, not individual blame.