

# Privacy Boundaries

Public / pilot-facing

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 scoring	No automated discipline	Human review required

## 2. What Aware Mate is for - and not for

<p><b>Aware Mate can</b></p> <ul style="list-style-type: none"> <li>• Prompt locally when sustained watchkeeping patterns need attention.</li> <li>• Generate derived event metadata and aggregated review outputs.</li> <li>• Support procedure, training, workload and pilot close-out review by authorised humans.</li> </ul>	<p><b>Aware Mate is not for</b></p> <ul style="list-style-type: none"> <li>• Live CCTV or remote bridge surveillance.</li> <li>• Identifying, ranking or scoring individual officers.</li> <li>• Emotion, stress, intent or personality inference.</li> <li>• Automated HR, discipline, blame or fitness-for-duty decisions.</li> <li>• Navigation control or ECDIS/radar/autopilot control.</li> </ul>
--	---

## 3. Default shore review

<p><b>Standard shore review may include</b></p> <ul style="list-style-type: none"> <li>• Period-level alert trends and severity mix.</li> <li>• Valid monitoring time and pilot KPI summary.</li> <li>• Alert load per monitored hour.</li> <li>• Aggregated long-absence flags, if enabled.</li> <li>• Context-weighted review, if agreed and available.</li> </ul>	<p><b>Standard shore review does not include</b></p> <ul style="list-style-type: none"> <li>• Continuous raw video feed or raw video ashore by default.</li> <li>• Officer identity, face identity or biometric profiles.</li> <li>• Exact event timestamps in basic aggregated review.</li> <li>• Automated conclusions about fault, intent or performance.</li> </ul>
--	---

## 4. 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.

## 5. Pilot governance commitments

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