

PUBLIC POLICY

Data Protection & Privacy Policy

How ELNAV.AI handles personal data across its website, business activities, research, pilots and maritime systems.

Organisation: ELNAV.AI d.o.o.

Version: 2.0

Effective date: 30 July 2026

Policy owner: Founder & Chief Executive Officer

Review cycle: At least annually and after material legal, organisational or technical change

1. Purpose and scope

ELNAV.AI develops maritime safety, training and intelligence systems. This policy explains how personal data are handled across the company, including the website, enquiries, in-house business development, recruitment, research, demonstrations, pilots, technical support and product operation.

It applies to all current and future ELNAV.AI products and projects. Where a specific pilot, study, customer deployment or employment activity needs more detailed information, a project-specific notice, agreement or consent form supplements this policy and takes precedence for that activity.

ELNAV.AI applies Regulation (EU) 2016/679 (GDPR), the Croatian Act on the Implementation of the GDPR and other applicable data-protection requirements. References to the EU AI Act describe related governance commitments and do not replace a case-by-case legal assessment.

2. Controller and roles

ELNAV.AI d.o.o., Technology Park Split, Dračevac 3D, 21000 Split, Croatia, is the controller for personal data processed for its own website, administration, recruitment, research and business-development purposes. Contact: info@elnav.ai.

For customer-operated systems, ELNAV.AI may act as a processor, joint controller or independent controller depending on who determines the purposes and means of processing. The applicable agreement and deployment notice define those roles.

3. Data we process, purposes and legal bases

3.1 Website, enquiries and communications

We may process names, professional contact details, company details, messages, meeting records and limited technical data such as IP address, browser data and security logs. We use these data to answer enquiries, arrange meetings, provide requested material, protect the website and take steps toward a contract.

The legal basis may be steps taken at the person's request before a contract, performance of a contract, legitimate interests in managing professional communications and website security, or consent for non-essential cookies and communications where consent is required.

3.2 In-house B2B outreach

ELNAV.AI manages its B2B outreach campaign in-house. We may identify relevant professional contacts through company websites, public registers, event materials, professional networking platforms, referrals and reputable business-information sources.

The data are limited to professional information such as name, role, organisation, business contact details, source, relevant public professional context, communication history and objection status. We use them to contact organisations about maritime products, pilots, partnerships, procurement or relevant events.

The legal basis is ELNAV.AI's legitimate interest under Article 6(1)(f) GDPR in developing relevant business relationships. Before contact, we consider role relevance, reasonable expectations and the likely impact on the individual. At or before the first communication, recipients receive clear information about ELNAV.AI and a simple way to object. We stop active outreach after an objection and may retain only the minimum suppression record needed to respect it.

The campaign is directed to professional roles and organisations, not consumer marketing. ELNAV.AI does not sell B2B contact data.

3.3 Recruitment and workforce administration

We may process application materials, interview notes, professional qualifications, employment and payment records, attendance or leave information, training records and other data needed to recruit and manage personnel. Legal bases include pre-contractual steps, contract performance, legal obligations and legitimate interests in operating the company.

3.4 Research, demonstrations and pilots

Depending on the approved protocol, we may process video or images, audio or voice, speech transcripts, facial or body landmarks that are not used for identification, derived watchkeeping or interaction events, system and sensor logs, timestamps, device identifiers, vessel or scenario context, survey responses and technical performance data.

These data are used to develop, test, validate, troubleshoot and document system behaviour. The legal basis is defined for each activity and may include consent, contract, legitimate interests or another lawful basis. If special-category data are involved, processing begins only after an applicable Article 9 GDPR condition and safeguards have been documented.

Video, voice and facial landmarks are not automatically biometric data under the GDPR. They are treated as biometric special-category data when specific technical processing is used for the purpose of uniquely identifying a person. ELNAV.AI's current watchkeeping systems are not designed for identity recognition.

3.5 Product operation and support

Product and support data may include configurations, derived alerts or events, acknowledgement records, assessment or training records, diagnostic logs, system-health information and relevant vessel, sensor or scenario context. Purposes include providing the service, system security, troubleshooting, quality assurance and agreed reporting.

4. Product privacy boundaries

4.1 Aware Mate

1. Processing is performed on board by default.
2. The system is not designed for identity recognition or emotion recognition.
3. Raw video is not sent ashore by default.
4. Outputs are advisory and are intended to support active watchkeeping, not medical diagnosis, psychological assessment or automated discipline.

4.2 Speech-based bridge systems

Helm-order and checklist-related systems may process bridge speech, transcripts and ship-sensor context. Speaker identification is not required for the intended verification function. Raw audio storage is not enabled by default unless an approved research, testing, quality or incident-review purpose requires it and the applicable notice, access controls and retention period are defined.

4.3 OSC Training

OSC Training may process participant identifiers, scenario events, trainer observations, scores, timestamps, reports and, where specifically agreed, audio or video evidence. It supports operational training assessment and debriefing. The training operator and ELNAV.AI define their respective roles, access and retention in the applicable agreement.

4.4 Other projects

Navigation, resilient-PNT, traffic-intelligence and environmental projects may process vessel, sensor, location and operational data. Personal data are included only when necessary for a defined purpose and are subject to the same minimisation, access and retention controls.

5. Data-protection principles

5. **Purpose limitation.** We define why data are needed before collection and do not use them incompatibly.
6. **Data minimisation.** We collect and retain only data reasonably necessary for the stated purpose.
7. **Privacy by design and default.** Local processing, derived outputs, restricted access and non-identifying data are preferred where practical.
8. **Accuracy.** We provide reasonable ways to correct inaccurate personal data.
9. **Storage limitation.** Retention is defined by purpose, contract, law and documented risk.
10. **Accountability.** Higher-risk activities receive documented review, including a data-protection impact assessment where required.

6. Retention

Retention is determined by the activity rather than one blanket period:

11. **Business and contract records.** Retained for the relationship and any statutory accounting, tax, grant, audit or legal period.
12. **B2B outreach.** Reviewed periodically and removed when no longer relevant; a minimal suppression record may remain after objection.
13. **Unsuccessful applications.** Retained only for the recruitment process and a limited defence period, unless the applicant agrees to a longer talent-pool period.
14. **Research and pilots.** Defined in the protocol, notice, consent form or agreement. Raw media are not retained by default.
15. **Operational and diagnostic data.** Retained only for agreed service, safety, support, investigation or reporting needs.
16. **Website and security logs.** Retained for a limited period proportionate to security and troubleshooting needs.

7. Recipients, processors and transfers

Access is limited to authorised personnel and, where necessary, customers, project partners, professional advisers, IT, hosting, communications, analytics, research or technical service providers. Processors are engaged under appropriate contractual and confidentiality terms.

If personal data are transferred outside the European Economic Area, ELNAV.AI uses an adequacy decision or appropriate safeguards such as the European Commission's Standard Contractual Clauses, together with supplementary measures where needed.

8. Cookies and similar technologies

The website uses necessary cookies for security and core functionality. Non-essential analytics, embedded media, marketing pixels or similar technologies are activated only on the basis shown in the cookie banner, including consent where required. The banner provides current cookie categories, providers and durations and allows users to change their choices.

9. Security and incident management

ELNAV.AI applies technical and organisational measures proportionate to the data and risk. These may include role-based access, least-privilege permissions, encryption in transit and at rest where appropriate, secure configuration, patching, backups, logging, confidentiality duties, supplier review and controlled deletion.

Suspected personal-data incidents are assessed promptly. ELNAV.AI notifies the competent supervisory authority and affected individuals when the GDPR requires it.

10. Individual rights

Depending on the processing and legal basis, individuals may request access, rectification, erasure, restriction, portability or information about their data, and may object to processing based on legitimate interests. Consent can be withdrawn at any time without affecting earlier lawful processing. Requests can be sent to info@elnav.ai.

Individuals may lodge a complaint with the Croatian Personal Data Protection Agency (AZOP), Selska cesta 136, 10000 Zagreb, Croatia, azop@azop.hr, or another competent supervisory authority.

11. Automated decisions and human oversight

ELNAV.AI systems are designed to provide advisory, technical, training or situational-support outputs. ELNAV.AI does not use them by default to make solely automated decisions that produce legal or similarly significant effects on individuals. Any materially different use requires separate assessment, transparency and safeguards.

12. Governance, updates and contact

The CEO is accountable for this policy and may designate operational owners for individual projects. Processing records, notices, agreements and risk assessments are maintained at a level proportionate to the activity and stage of development.

Privacy questions and rights requests: info@elnav.ai. General company information: <https://elnav.ai>.

Document history

Version	Change
Version 1.0	Original public document.
Version 2.0	30 July 2026. Rewritten for the current portfolio and organisation; removed the obsolete external outreach-agency and plugin references; added in-house B2B outreach, product-specific privacy boundaries, controller/processor roles, retention criteria and corrected biometric-data wording.

Approval

This policy is approved by the Founder & Chief Executive Officer and applies from the effective date shown above.

Approved by: Hrvoje Mihovilović

Role: Founder & Chief Executive Officer

Date: 30 July 2026

Signature: 