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:** 2.1
**Approval date:** 24 September 2026
**Effective date:** 24 September 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 defines the processing for that activity. It must remain consistent with applicable law and the product privacy boundaries in section 4.

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. Where ELNAV.AI acts as a processor, it processes personal data on documented controller instructions.

# 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.

Where a documented assessment supports it, the legal basis is ELNAV.AI's legitimate interest under Article 6(1)(f) GDPR in developing relevant business relationships. The assessment considers necessity, role relevance, reasonable expectations and the likely impact on the individual. Applicable electronic-marketing rules are assessed separately; consent is obtained where required. A B2B label is not a blanket exemption.

At or before the first communication, recipients receive clear information about ELNAV.AI, the relevant processing and a simple way to object. We stop direct-marketing processing after an objection and may retain only the minimum suppression record needed to respect it. The campaign targets 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.

### 3.4 Research, demonstrations and pilots (continued)

Video, voice and facial landmarks may be personal data even without identity recognition. Biometric data under Article 4(14) GDPR involve specific technical processing of physical, physiological or behavioural characteristics that allows or confirms unique identification. Article 9 separately covers biometric data processed for the purpose of uniquely identifying a person. Other special-category data, such as health data, require their own assessment. 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.

### 3.6 Internal document storage and controlled copying

ELNAV.AI uses its Zoho business environment for business documentation, alongside authorised workstations. Records may contain contact, contractual, financial, personnel or project information. A separate personal Google Drive account with a Google One subscription is also used for file storage. Business use of that account requires a defined, approved scope; it is not designated as the company's primary business repository. The legal basis follows the underlying activity; copying does not authorise a new use.

Rclone is the selected locally operated tool for planned scheduled copying to Google Drive. It uses the Google Drive API to list, compare and transfer approved files and metadata. As at 24 September 2026, configuration is in progress and unattended copying is not yet active. Transfers run between the authorised workstation and the selected storage provider; rclone is not a separate hosted storage service.

Before automated copying is enabled, its owner must define the source and destination, permitted data, exclusions, access rights and retention. A mixed personal or work download folder is not approved as a whole merely because it can be copied. Restricted customer records, personal material and raw media require a separate justification and any necessary permission before inclusion. This workflow is separate from on-board processing and does not authorise raw bridge-media export.

## 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.

Where shore reporting is agreed, aggregated outputs are preferred. Removing names does not by itself make data anonymous: timestamps, watch rosters and small crew groups can allow indirect identification. Additional detail or media access requires documented purpose, authority, access controls and retention rules.

# 4. Product privacy boundaries (continued)

## 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.

## 6. Retention (continued)

The operational retention schedule must identify the owner, period or objective deletion criteria, review trigger and relevant storage locations for each category. The applicable notice must give the retention period or criteria for the processing concerned. This includes cloud copies, transfer logs, exported reports and backups, not only the original working file.

Deleting a local file or revoking an application connection does not necessarily delete separate copies. Rclone's copy mode does not delete destination-only files and may replace changed files at the same path. Retention review must include copies already uploaded manually. Deletion requests, expiry and legal holds must be assessed across relevant copies. Backup deletion must follow a documented expiry and restoration process; recovery-only data must not be routinely reused or restored contrary to a valid deletion decision.

## 7. Recipients, processors and transfers

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

Zoho and Google services are assessed separately against their actual account, service, contractual roles, required data-processing terms, access controls and storage or remote-access locations. A Google One subscription or Google Cloud OAuth project does not by itself establish Google Workspace data-processing terms. Personal-data copying to a destination must not be enabled until required contractual safeguards are in place. Permissions must be limited to what is necessary; technical access does not authorise wider use or public sharing.

For internal tools using Google APIs, use of information received through those APIs must follow the applicable Google API user-data policies, including Limited Use requirements. File-management access does not authorise unrelated advertising, data sale or general-purpose model training. Separate access by another application or AI tool requires its own purpose, permissions and privacy review.

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. The relevant notice identifies the applicable transfer arrangement and how information about safeguards can be obtained.

## 8. Cookies and similar technologies

The website may use necessary cookies for security and core functionality. Where non-essential analytics, embedded media, marketing pixels or similar technologies are used, they must remain inactive until valid consent is obtained where required. Refusing non-essential cookies must not prevent access to basic website content.

The cookie notice and consent controls must reflect the technologies actually deployed, including their purposes, providers and durations. Visitors must be able to accept or reject non-essential cookies with equal ease and change or withdraw their choices. Publishing this policy does not establish that a particular banner or website configuration has been technically verified.

## 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.

Access rights must be reviewed when personnel join, change roles or leave. Obsolete permissions, shared links, device access and authentication tokens must be withdrawn or replaced as appropriate. Copying tools must not change sharing permissions unless separately authorised. Credentials and logs must be access-controlled and must not be placed in public documents or repositories.

Suspected personal-data incidents are assessed promptly. ELNAV.AI notifies the competent supervisory authority and affected individuals when the GDPR requires it. Where ELNAV.AI acts as processor, it notifies the controller without undue delay after becoming aware of a personal-data breach.

## 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.

Requests are addressed without undue delay and normally within one month of receipt. Where a lawful extension is needed, the individual is informed within the first month of the extension and reasons. Identity verification is limited to what is necessary. Direct-marketing objections are respected without requiring a reason.

Individuals may lodge a complaint with the Croatian Personal Data Protection Agency (AZOP), Ulica Metela Ožegovića 16, 10000 Zagreb, Croatia, azop@azop.hr, or another competent supervisory authority. Current AZOP contact details are available at azop.hr.

## 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, and must not override the product boundaries in section 4.

## 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. Material changes to data flows, recipients, access or retention require review before activation.

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. |
| **Version 2.1** | 24 September 2026. Added controlled internal storage and copying; confirmed Zoho business storage, the separate personal Google Drive / Google One account and rclone as the selected tool for planned copying. Clarified copy-retention, service-review, electronic-marketing, biometric-data, indirect-identification, cookie, access-change and rights-handling wording; updated AZOP contact details. Product privacy boundaries are unchanged. Approved and effective on this date. |

# Approval

Version 2.1 is approved by the Founder & Chief Executive Officer and takes effect on 24 September 2026, superseding version 2.0. Publication and operational implementation must reflect the approved text and the actual processing arrangements.

**Approved by:** Hrvoje Mihovilović

**Role:** Founder & Chief Executive Officer

**Date:** 24 September 2026

**Signature:**