NAVIO

Privacy Policy

Navio LLC · naviopro.ai
Effective date: ● 2026 · Last updated: 20 October 2026
Applies to: Consumer (B2C) users, Institutional (B2B) users, Institution staff, website visitors

Contents

1. About this Policy
2. Our Role: Controller or Processor
3. Personal Data We Collect
4. How We Use Your Data and Our Legal Bases
5. How Navio’s AI Works and How We Protect Your Data in It
6. How We Share Personal Data
7. Student Records and Education-Sector Laws (US)
8. Institution Staff, Advisors and Business Contacts
9. Children and Teenagers
10. Where We Store Data and International Transfers
11. How Long We Keep Data
12. Your Rights
13. Security
14. Cookies and Similar Technologies
15. Marketing Communications
16. Notice to US Residents (including California)
17. Other Countries
18. Changes to this Policy
19. Contact Us

Our core commitments

1. **We do not sell, rent or trade your personal data**, and we do not use it for targeted advertising.
2. **We do not use your CVs, chats, prompts, uploaded files or student records to train AI models** — ours or anyone else's. Our AI providers are contractually prohibited from training on them.
3. **Navio's AI recommends; people decide.** We do not make decisions about you that have legal or similarly significant effects based solely on automated processing.
4. **Your data is hosted in the European Union** (AWS, Frankfurt, Germany) unless your institution or local law requires another location.
5. **Institutional data stays with the institution.** When you use Navio through your university, college or school, that institution controls your data and we act only on its instructions.
6. **You can delete your account and data at any time.** Deletion removes your profile, chat history and files from our live systems; backups are overwritten on a rolling cycle.

1. About this Policy

This Privacy Policy explains how **Navio LLC** ("**Navio**", "**we**", "**us**", "**our**") collects, uses, shares and protects personal data when you use the Navio website at naviopro.ai, the Navio web and mobile applications, the Navio AI career guidance tools (including AI Chat Mentor, CV Review & Builder, AI Interview Prep, Job and Scholarship Search, AI Prompting Tutor, Coaching Center and job simulations), the Navio advisor and administrator tools, and any related services (together, the "**Services**").

Navio LLC is a limited liability company organised under the laws of the State of Wyoming, USA, with its registered address at 30 N Gould St, Ste R, Sheridan, WY 82801, USA.

This Policy is written to meet the requirements of the EU General Data Protection Regulation ("**EU GDPR**"), the UK GDPR and Data Protection Act 2018 as amended by the Data (Use and Access) Act 2025 ("**UK GDPR**"), the Swiss Federal Act on Data Protection, US federal and state privacy and student-privacy laws (including FERPA, COPPA, the California Consumer Privacy Act as amended by the CPRA ("**CCPA**") and SOPIPA), the Republic of Kazakhstan Law No. 94-V "On Personal Data and their Protection", and other laws listed in Section 17. Where a local law gives you stronger rights than this Policy, the local law applies.

Please also read our Terms of Service. If you do not agree with this Policy, please do not use the Services.

2. Our Role: Controller or Processor

Navio is offered in two ways. Our role under data protection law differs between them:

How you use Navio	Who is responsible for your data	Which privacy notice governs
Directly — you create a personal Navio account yourself ("**Consumer**" or "**B2C**" use).	**Navio is the controller.** We decide why and how your data is processed.	This Policy.
Through an institution — your university, college, school, bootcamp, employer or other organisation (an "**Institution**") gives you access, including white-labelled versions that show the Institution's brand ("**Institutional**" or "**B2B**" use).	**The Institution is the controller; Navio is its processor** (in US terms, a "service provider" and, for US schools, a "school official" under FERPA). We process data only on the Institution's documented instructions under a Data Processing Agreement.	Your Institution's privacy notice. This Policy describes how Navio handles the data for the Institution and applies to the limited processing for which Navio is itself controller (see below).

How you use Navio	Who is responsible for your data	Which privacy notice governs
Visiting our website, contacting us or attending our events (including Institution staff, prospective customers and partners).	**Navio is the controller.**	This Policy.

Even in Institutional use, Navio is an independent controller for a narrow set of activities: keeping the Services secure and preventing abuse; maintaining billing and contract records with the Institution; complying with our own legal obligations; and creating aggregated, de-identified statistics that cannot identify you or your Institution (Section 6.4). If you use Navio through an Institution, please send requests about your data to your Institution first; if you contact us, we will forward the request to the Institution and assist it.

If you have both a personal account and an Institutional account, they are kept separate. Data from your Institutional account is never moved into your personal account (or the reverse) unless you export it yourself or your Institution permits it.

3. Personal Data We Collect

3.1 Data you give us

Category	Examples
Account and identity data	Name, email address, password (stored only as a salted hash), phone number (optional), country, preferred language, age range or date of birth (to check eligibility), profile photo (optional).
Education and career profile	Institution, programme, year of study, courses, grades you choose to enter, skills, interests, career goals, work preferences, work history, projects, certifications, languages, career assessment answers.
CVs, cover letters and documents	Files and text you upload or create with CV Review & Builder, including any personal data they contain.
AI interactions (“Prompts” and “Outputs”)	Messages, questions and instructions you send to Navio’s AI tools, your interview-practice answers (text and, if you choose voice features, audio), simulation choices, and the responses, recommendations and feedback generated for you.
Job, scholarship and application activity	Roles or scholarships you view, save or apply for, application status you record, and deadlines.
Communications	Messages with advisors (Institutional use), support requests, survey responses and feedback.
Payment data (Consumer use)	Plan, purchase history, token balance and billing country. Card details are collected and processed directly by our payment provider; Navio does not see or store full card numbers.
Parent or guardian data	Where a user is a minor, the parent or guardian’s name, email and confirmation of consent (Section 9).
Business contact data	Name, job title, institution, work email and phone of Institution staff, prospects and partners; notes from demos and calls.

3.2 Data we collect automatically

Category	Examples
Device and log data	IP address, browser and device type, operating system, time zone, pages and features used, timestamps, error and crash logs. Personal content (names, emails, CV text, Prompts) is masked before entering our technical logs.
Cookies and similar technologies	Strictly necessary cookies (login, security, load balancing) and, only with your consent where required, analytics cookies. See Section 14.
Usage and engagement data	Feature usage, session length, completion of modules, and — in Institutional use — engagement indicators visible to authorised advisors (for example, last activity date).

3.3 Data we receive from others

- **Your Institution** (Institutional use): roster and enrolment data such as name, student ID, institutional email, programme, year, cohort and, where the Institution chooses to provide it, academic or career-service records, plus advisor notes and assignments.
- **Single sign-on providers** (for example, your Institution's identity provider, Google or Microsoft): your name, email and a unique identifier, if you choose to sign in this way.
- **Integrations you or your Institution connect** (for example, a learning-management or careers platform): only the data the integration is configured to share.
- **Public and licensed labour-market sources**: job postings, skill requirements, salary ranges and aggregated, de-identified career-pathway statistics. These datasets are used to build recommendations and do not identify you.
- **Payment provider**: confirmation of payment, refunds and fraud-risk signals.

3.4 Special category and sensitive data

Navio does not need, and asks you not to provide, information about your racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic or biometric data, health, sex life or sexual orientation, criminal convictions, government ID numbers (such as passport, National Insurance, Social Security or IIN numbers) or financial account details ("**Sensitive Data**").

Our systems are designed to detect and redact common direct identifiers and government ID numbers in CVs and Prompts before they are sent to AI providers (Section 5). If you choose to include Sensitive Data — for example, to ask for advice on requesting a disability-related workplace adjustment — we will process it only to answer your request, only with your **explicit consent** (which you give by choosing to include it after being shown a clear notice in the product), and never for profiling, analytics or any other purpose. You can withdraw consent by deleting the content. In Institutional use, the Institution determines whether and how Sensitive Data may be processed.

We do not use voice or video data to identify you biometrically, and **Navio does not perform emotion recognition** or infer emotions, personality traits or protected characteristics from your voice, face, writing or behaviour.

4. How We Use Your Data and Our Legal Bases

For users in the UK, EEA and Switzerland, we must have a legal basis for each use of personal data. The table below applies to Consumer use and to activities for which Navio is controller. In Institutional use, the Institution determines the legal basis (typically public task, legitimate interests or contract) and we act on its instructions.

Purpose	Data used	Legal basis (UK/EU GDPR)
Create and manage your account; authenticate you	Account, device data	Contract (Art. 6(1)(b))
Provide the AI career guidance features you request: chat mentor, CV review and building, interview practice, job and scholarship matching, simulations, coaching modules	Profile, CVs, Prompts and Outputs, activity	Contract (Art. 6(1)(b)). Where Sensitive Data is included: explicit consent (Art. 9(2)(a))
Remember context between sessions ("Guidance with memory")	Profile, Prompts and Outputs	Contract. You can view and clear memory at any time
Process payments, manage subscriptions and tokens, prevent payment fraud	Payment, account data	Contract; legal obligation (tax and accounting); legitimate interests (fraud prevention)
Customer support and service communications (security alerts, changes to terms, renewal reminders)	Account, communications	Contract; legal obligation
Keep the Services secure, detect abuse, enforce our Terms, debug errors	Device and log data (masked), account data	Legitimate interests (Art. 6(1)(f)) in a secure, reliable service; legal obligation
Improve and develop the Services using **aggregated or de-identified** usage statistics (Section 6.4)	Usage data, de-identified outputs ratings	Legitimate interests in improving our product. Never raw CVs, chats or student records
Marketing emails about Navio (Consumers)	Name, email	Consent where required; otherwise legitimate interests with an opt-out in every message
B2B sales and relationship management with Institutions and prospects	Business contact data	Legitimate interests (direct marketing to organisations, as recognised by the UK Data (Use and Access) Act 2025); opt-out at any time
Optional analytics cookies	Device and usage data	Consent (UK PECR / EU ePrivacy rules)
Parental consent for minors	Parent/guardian data	Legal obligation (COPPA where applicable) and consent
Opt-in "Talent visibility" — sharing your profile with employers or partner organisations you choose (if offered)	Profile, CV, selected outcomes	Consent (Art. 6(1)(a)), given separately for each programme and withdrawable at any time
Comply with law, respond to lawful requests, establish or defend legal claims	Any relevant data	Legal obligation; legitimate interests

Where we rely on **legitimate interests**, we have balanced our interests against your rights; you may ask us for details and you have the right to object (Section 12). Where we rely on **consent**, you may withdraw it at any time without affecting the lawfulness of earlier processing; withdrawing consent to optional features never prevents you from using the core Services.

You are not required by law to provide personal data. However, the data marked as necessary in the product (such as an email address to create an account) is required to provide the Services.

5. How Navio's AI Works and How We Protect Your Data in It

5.1 What the AI does

Navio uses large language models ("**LLMs**") supplied by third-party AI providers, combined with our own software, rules, prompts and labour-market data, to generate career guidance: explanations, suggested career paths, skills-gap analyses, CV feedback, interview feedback, ranked lists of jobs or scholarships and learning plans. Every recommendation is accompanied by the reasons behind it, and you can change or ignore any step.

You are always told when you are interacting with an AI system, and AI-generated content is labelled as such, in line with Article 50 of the EU AI Act.

5.2 Safeguards before data reaches an AI provider

- **Minimisation and redaction.** A server-side filter removes or replaces direct identifiers — names, email addresses, phone numbers, street addresses, government ID numbers and similar — with placeholders before your CV or Prompt is sent to an AI provider, wherever the task does not require them.
- **Business API only.** We use AI providers only through their enterprise/developer APIs under a data processing agreement — never consumer chat apps.
- **No training.** Our contracts and account settings prohibit AI providers from using Navio data to train or improve their models.
- **Limited retention by providers.** AI providers may keep API inputs and outputs only for the period stated in their agreements, and in any case no longer than 30 days, solely to provide the service and detect abuse; where zero-data-retention is available to us, we use it.
- **Location.** We use EU or other regional processing endpoints where the provider offers them. Where processing takes place outside the UK/EEA, the transfer is protected as described in Section 10.
- **Tenant isolation.** Each Institution's data is logically separated from every other Institution's and from Consumer data, with access controls preventing data from one environment appearing in another.

5.3 No training on your content

We do not use your CVs, cover letters, Prompts, Outputs, uploaded files, advisor notes or Institutional records to train, fine-tune or otherwise build AI models, whether ours or a third party's. When an advisor or user overrides a recommendation in Institutional use, that signal is used only to improve recommendations within that Institution's own environment, unless it has first been aggregated and de-identified as described in Section 6.4. If we ever wish to change this, we will ask for your separate, opt-in consent first (and, for Institutional data, the Institution's written instruction); refusing will not affect your use of Navio.

5.4 Automated decision-making and profiling

Navio analyses your profile to personalise guidance — this is profiling. However, **Navio does not make decisions based solely on automated processing that produce legal or similarly significant effects on you** (within Article 22 of the EU GDPR or the UK GDPR as amended). In particular, Navio does not decide admissions, grades, scholarship awards, disciplinary matters, eligibility for services, hiring or rejection. Recommendations are suggestions for you, your advisor or your Institution to consider.

In Institutional use, advisors may see indicators such as "may need support" based on engagement and progress. These indicators are designed to prompt human outreach, are reviewed by a person before any action, and are never used by Navio to deny a student a service or opportunity. Our Institutional terms prohibit Institutions from using Navio to make solely automated significant decisions about individuals.

You may ask how a recommendation was produced, request human review of any AI output by contacting your advisor (Institutional use) or us (Consumer use), and express your point of view or contest an outcome.

5.5 Accuracy, fairness and limits

AI output can be incomplete, outdated or wrong. Navio guidance is informational and is not a guarantee of admission, employment, salary or any outcome, and it is not legal, financial, immigration, medical or psychological advice. Please check important information (for example, application deadlines or visa rules) with the original source.

We test our AI features before release and periodically afterwards for accuracy and for unjustified differences in outputs across groups (for example, by gender, age or ethnicity, using synthetic test profiles rather than real users' protected characteristics), keep a record of these reviews, and correct issues we find. Where required, we carry out and maintain Data Protection Impact Assessments for our AI processing.

6. How We Share Personal Data

We share personal data only as described below. **We do not sell personal data and do not "share" it for cross-context behavioural advertising** (as those terms are defined in US state privacy laws).

6.1 Service providers (sub-processors)

We use carefully selected providers who process data on our behalf under written contracts that require confidentiality, security and use only on our instructions. Our current key providers are:

Provider	Purpose	Data location
Amazon Web Services (AWS EMEA SARL / Amazon Web Services, Inc.)	Cloud hosting, databases, file storage, backups	EU — Frankfurt, Germany (eu-central-1)
OpenAI, L.L.C. / OpenAI Ireland Ltd (API)	Large language model processing	EU endpoint where available; otherwise USA
Anthropic, PBC / Anthropic Ireland Ltd (API)	Large language model processing	EU endpoint where available; otherwise USA
Stripe	Payments, subscriptions, fraud prevention	EU/USA/ALL
Resend Inc	Transactional and service emails	USA (data storage); email sending from Ireland (eu-west-1)
PostHog, Inc.	Product analytics (consent-based where required)	Germany (AWS Frankfurt, eu-central-1) via PostHog Cloud EU; some PostHog sub-processors in the EU

The up-to-date list of sub-processors is published at naviopro.ai/subprocessors. Institutions receive advance notice of new sub-processors and may object as set out in their agreement. Payment providers may act as independent controllers for some payment and fraud data under their own privacy notices.

6.2 Your Institution

In Institutional use, authorised staff of your Institution (for example, career advisors and administrators) can see your profile, activity, outputs and progress to the extent the Institution has configured, so they can support you. Role-based permissions limit advisors to their assigned students. Navio staff hold no

standing access to Institutional records; support access requires the Institution's request or approval, is time-limited and is logged.

6.3 People and organisations you choose

If you choose to share content — for example, send your CV to an employer, connect an integration, or opt in to a "Talent visibility" programme — we share the data you select with the recipient you select. Recipients handle it under their own privacy policies. You can withdraw from such programmes at any time; this stops future sharing.

6.4 Aggregated and de-identified information

We may create statistics that cannot reasonably be used to identify any individual or Institution (for example, "the share of users who completed interview practice before applying") and use or publish them to improve the Services, benchmark outcomes and report on our impact. We take reasonable measures to ensure such data cannot be re-identified, we publicly commit not to attempt re-identification, and we contractually require any recipients to do the same. Institutional data is included only in a form that cannot identify the Institution, unless the Institution agrees otherwise.

6.5 Legal, safety and corporate reasons

- To comply with law, a court order or a lawful request by public authorities; we will challenge requests we believe are overbroad and, where lawful, notify the affected Institution or user.
- To protect the rights, safety or property of users, Navio or others, including to prevent fraud or address an imminent risk of harm.
- To professional advisers (lawyers, accountants, auditors) under confidentiality obligations.
- In connection with a merger, acquisition, financing or sale of assets, subject to confidentiality and to this Policy continuing to protect your data; Institutional data will be handled as required by the Institution's agreement. We will notify you before your data becomes subject to a different privacy policy.

7. Student Records and Education-Sector Laws (US)

When a US school, college or university uses Navio, we act as a "school official" with a legitimate educational interest under the Family Educational Rights and Privacy Act (**FERPA**), under the direct control of the Institution with respect to education records. We use education records only to provide the Services to the Institution, do not re-disclose them except as the Institution directs or the law requires, and return or delete them at the end of the contract.

For K–12 schools, we comply with the Children's Online Privacy Protection Act (**COPPA**), California's Student Online Personal Information Protection Act (**SOPIPA**) and similar state student-privacy laws. In particular, we do not use student data for targeted advertising, do not build profiles of students for non-educational purposes, do not sell student data, and do not disclose it except as these laws allow. We are willing to sign state-specific student data privacy agreements (for example, the Student Data Privacy Consortium's National Data Privacy Agreement) and New York Education Law §2-d riders.

8. Institution Staff, Advisors and Business Contacts

If you are an advisor or administrator using Navio on behalf of an Institution, we process your account, usage and activity data to provide the Services to your Institution and to keep them secure. If you are a prospective customer or partner, we process your business contact data to respond to you, send relevant information and manage our relationship. You can unsubscribe from marketing at any time using the link in each email or by contacting us.

9. Children and Teenagers

Age	Consumer (direct) use	Institutional use
Under 13	Not permitted. We do not knowingly collect personal data from children under 13 through Consumer accounts and will delete it if we learn we have.	Permitted only where the school or Institution authorises use for an educational purpose and provides any consent required by law (including COPPA school authorisation); data is used only for that educational purpose.
13 to 17 (or under the age of digital consent in your country, which in parts of the EU is up to 16)	Permitted only with verified consent of a parent or legal guardian, who must also make any purchases. The parent or guardian can review, correct or delete the teen's data at any time.	Permitted under the Institution's authority and policies.
18 and over	Permitted.	Permitted.

For users under 18, we apply high-privacy defaults consistent with the UK Age Appropriate Design Code: profile visibility and any "Talent visibility" features are off and cannot be enabled by the minor alone; marketing is off; we do not use nudge techniques to encourage minors to share more data or weaken privacy settings; and safety guardrails in our AI tools are tuned for younger users. If you believe a child has provided us with personal data without proper consent, contact us at info@naviopro.ai and we will delete it.

10. Where We Store Data and International Transfers

Our primary hosting is in the European Union (AWS, Frankfurt, Germany), including databases, file storage and backups. We do not replicate production data to regions outside the EU unless an Institution or applicable law requires a specific location. Where local law requires data about its residents to be stored in-country (for example, the Republic of Kazakhstan), the primary copy of that data is stored on servers in that country.

Navio LLC is a US company, and some providers (for example, AI providers) may process data in the United States or other countries. When personal data from the UK, EEA or Switzerland is transferred to a country without an adequacy decision, we rely on appropriate safeguards: the EU Standard Contractual Clauses, the UK International Data Transfer Addendum, the Swiss addendum, and/or the recipient's certification under the EU–US Data Privacy Framework and its UK and Swiss extensions, together with supplementary measures such as encryption and redaction. You can request a copy of the relevant safeguards by contacting us.

11. How Long We Keep Data

Data	Retention period
Consumer account, profile, CVs, Prompts and Outputs	While your account is active. You can delete individual items or memory at any time. If your account is inactive for 24 months, we will warn you and then delete it.
Deleted accounts	Removed from live systems within 30 days of your request; residual copies in encrypted backups are overwritten within a further 35 days.
Institutional data	As instructed by the Institution. At the end of the contract, returned or deleted within 30 days (backups as above), unless the Institution instructs otherwise or law requires retention.

Data	Retention period
AI provider copies of Prompts and Outputs	Zero retention where available; otherwise no more than 30 days, for abuse monitoring only.
Technical and security logs (masked)	Up to 90 days; up to 12 months for security-incident investigation records.
Payment, invoice and tax records	As required by tax and accounting law — generally 7 years.
Support and communications	Up to 24 months after the request is closed.
Marketing preferences and suppression lists	Until you opt out; we keep a minimal record of the opt-out so we do not contact you again.
Parental-consent records	For as long as the minor's account exists plus 3 years.
Aggregated or de-identified statistics	May be kept indefinitely because they do not identify anyone.

12. Your Rights

12.1 Rights in the UK, EEA and Switzerland

Subject to conditions and exceptions in the law, you have the right to: **access** your personal data and receive a copy; **rectify** inaccurate data; **erase** your data; **restrict** processing; **data portability** (receive data you provided in a structured, machine-readable format, or have it sent to another provider); **object** to processing based on legitimate interests, and at any time to direct marketing; **withdraw consent** at any time; and not be subject to solely automated decisions with legal or similarly significant effects, and to obtain human intervention, express your view and contest such a decision.

Many of these rights can be exercised directly in your account settings (download, edit, clear memory, delete account). Otherwise, contact us at info@naviopro.a]. We will respond within one month (extendable by two further months for complex requests, in which case we will tell you why). We may need to verify your identity. Exercising your rights is free unless a request is manifestly unfounded or excessive.

You also have the right to complain to a supervisory authority — in the UK, the Information Commissioner's Office (ico.org.uk); in the EEA, the authority in your country of residence, work or the alleged infringement; in Switzerland, the FDPIC. We would appreciate the chance to address your concern first.

12.2 Institutional users

If you use Navio through an Institution, please make your request to the Institution, which decides how to respond. We will help the Institution respond promptly, including by providing tools for it to export, correct and permanently delete your data.

13. Security

We maintain a written information security programme appropriate to the sensitivity of the data, including: encryption in transit (TLS 1.2 or higher) and at rest (AES-256); logical isolation of each Institution's data; role-based access with least privilege and multi-factor authentication for staff; no standing staff access to Institutional records; logging and monitoring of access; masking of personal content in technical logs; secure software development and code review; vulnerability management and regular penetration testing; vendor security reviews; backup and disaster-recovery procedures; staff confidentiality obligations and training; and a documented incident-response plan. We have completed the EDUCAUSE Higher Education Community Vendor Assessment Toolkit (HECVAT), available to Institutions for review.

No system is perfectly secure. If we become aware of a personal data breach, we will notify the competent supervisory authority within 72 hours where required, affected Institutions without undue delay (and within the period set out in their agreement), and affected individuals where the law requires.

14. Cookies and Similar Technologies

We use strictly necessary cookies and local storage to log you in, keep the Services secure, remember your preferences and balance load; these do not require consent. With your consent where required (in the UK and EEA, through our cookie banner, where "Reject" is as easy as "Accept"), we also use analytics cookies to understand how the Services are used. **We do not use advertising or cross-site tracking cookies.** You can change your choices at any time through "Cookie settings" in the website footer. We honour Global Privacy Control (GPC) signals as a valid opt-out where required by law.

15. Marketing Communications

We send Consumers marketing emails only where permitted by law (with consent, or about similar Navio services you have used, with an easy opt-out). Every marketing message contains an unsubscribe link. We never send marketing to users we know to be under 18, and never send marketing to students using Navio through an Institution. Service messages (such as security notices and renewal reminders) are not marketing and will still be sent.

16. Notice to US Residents (including California)

This Section supplements the rest of this Policy for residents of US states with comprehensive privacy laws, including California, Colorado, Connecticut, Delaware, Iowa, Maryland, Minnesota, Montana, Nebraska, New Hampshire, New Jersey, Oregon, Tennessee, Texas, Utah, Virginia and others ("**US State Privacy Laws**"). Some of these laws apply only to businesses that meet certain thresholds; we apply the protections below to all US residents as a matter of policy. In Institutional use, Navio acts as a service provider/processor to the Institution, and requests should be directed to the Institution.

16.1 Categories of personal information (previous 12 months)

Category (CCPA)	Examples	Source	Disclosed for a business purpose to
Identifiers	Name, email, account ID, IP address	You; Institution; devices	Service providers; your Institution
Customer records (Cal. Civ. Code §1798.80)	Name, phone, education and employment history	You; Institution	Service providers; your Institution
Commercial information	Plans, purchases, token balance	You; payment provider	Payment and service providers
Internet or electronic network activity	Usage, feature interactions, logs	Devices	Service providers
Audio information	Voice answers in interview practice (if you use voice)	You	Service providers (speech processing)
Professional or employment-related information	Work history, skills, CV	You; Institution	Service providers; recipients you choose
Non-public education information (FERPA)	Programme, courses, grades provided	You; Institution	Service providers; your Institution

Category (CCPA)	Examples	Source	Disclosed for a business purpose to
Inferences	Career interests, skills gaps, suggested paths	Derived by the Services	Service providers; your Institution
Sensitive personal information	Account log-in credentials; any health data you choose to include	You	Service providers, only to provide the Services

We collect these categories for the purposes in Section 4 and retain them as described in Section 11. **We do not sell personal information or share it for cross-context behavioural advertising, and we have not done so in the past 12 months.** We do not knowingly sell or share personal information of consumers under 16. We use sensitive personal information only for purposes permitted by Cal. Code Regs. tit. 11, §7027(m) (such as providing the Services you request and security), so the right to limit does not apply; we do not infer characteristics from it.

16.2 Your US privacy rights

Depending on your state, you may have the right to: know and access the personal information we hold about you (including specific pieces and categories); correct inaccurate information; delete your information; obtain a portable copy; opt out of sale, "sharing", targeted advertising and profiling in furtherance of decisions that produce legal or similarly significant effects (we do not engage in these activities); limit use of sensitive personal information; and not be discriminated against for exercising your rights. Residents of some states may appeal our decision on a request by replying to our response; if the appeal is denied, you may contact your state Attorney General.

To make a request, email privacy@naviopro.ai or use request form URL. We will confirm receipt within 10 business days and respond within 45 days (extendable once by 45 days where permitted). We will verify your identity by matching information you provide with our records; for sensitive requests, we may ask for additional confirmation. You may use an authorised agent with written permission; we may ask you to verify your identity directly. Parents or guardians may make requests on behalf of minors.

16.3 Other US disclosures

- **Shine the Light (Cal. Civ. Code §1798.83):** we do not disclose personal information to third parties for their direct marketing purposes.
- **Do Not Track / GPC:** we treat a Global Privacy Control signal as a request to opt out where the law requires. Because we do not sell, share or use tracking for advertising, this has no further effect on the Services.
- **Minors in California:** registered users under 18 may request removal of content they posted by contacting us.
- **Washington, Nevada and other consumer-health laws:** we do not seek to collect consumer health data; any such data you choose to include is used only to respond to your request and never sold.

17. Other Countries

Navio is designed to meet the GDPR standard globally. Where you are located in another jurisdiction, the following also applies:

Jurisdiction	Additional points
Kazakhstan	Processing is based on your consent (or your Institution's lawful basis), which you may withdraw. Personal data of Kazakhstan residents is stored on servers located

Jurisdiction	Additional points
	in Kazakhstan as required by Article 12 of Law No. 94-V; cross-border transfers occur only as permitted by that law.
Other CIS countries (Uzbekistan, Kyrgyzstan, Azerbaijan, Georgia, Ukraine)	We obtain consent where local law requires it and comply with any local storage or registration requirements before launching services there.
Canada	We comply with PIPEDA and applicable provincial laws; you may access and correct your information and withdraw consent.
Australia / New Zealand	We comply with the Australian Privacy Principles and the New Zealand Privacy Act 2020, including breach notification.
Switzerland	The revised Federal Act on Data Protection (nFADP) applies; Swiss residents may complain to the FDPIC.
UAE, Saudi Arabia, Qatar	We comply with the applicable PDPL/PDPPL, including consent, transparency and transfer rules.
Brazil, Latin America	We comply with the LGPD and applicable national laws; Brazilian residents may contact our privacy team as our point of contact for the ANPD.
Asia-Pacific (Singapore, Malaysia, Thailand, Philippines, India)	We comply with the applicable PDPA / Data Privacy Act / DPDP Act, including consent and grievance mechanisms.

Before we offer the Services in a new country, we review local requirements (including any data-localisation, registration or representative obligations) and will update this Policy if additional terms apply.

18. Changes to this Policy

We may update this Policy to reflect changes in our Services or the law. We will post the new version with a new “Last updated” date and, for material changes, notify you by email or in the product at least 30 days before the change takes effect (or sooner where required by law or for security reasons). Where a change requires your consent — for example, any use of your content for AI training — we will ask for it and will not apply the change without it.

19. Contact Us

Controller	Navio LLC, 30 N Gould St, Ste R, Sheridan, WY 82801, USA
Privacy team / Data Protection Officer	info@naviopro.ai ·
UK representative (Art. 27 UK GDPR)	Assel Rabatova, Online office, uk-rep@naviopro.ai
EU representative (Art. 27 EU GDPR)	Daria Soloveva, Online office, eu-rep@naviopro.ai
Postal address for requests	Navio LLC, Attn: Privacy, 30 N Gould St, Ste R, Sheridan, WY 82801, USA