

Privacy policy

Version 2.1, effective 2026-10-25

1. Who we are

Nordic USV AS, organisation number 930 919 365, Thormøhlens gate 51, 5006 Bergen, Norway, runs the website nordicusv.com and [Kystdata.io](https://kystdata.io), an oceanographic data platform. You can reach us at info@nordicusv.com.

This policy covers both the website and the platform. Section 4 is about the website only, and section 5 only about the AI features in the platform.

[Kystdata.io](https://kystdata.io) is a business service. It is not directed at private individuals creating accounts for personal use.

The measurement data itself (water quality readings, sensor data, positions of survey equipment) is environmental data about the sea, not personal data. Personal data enters the platform mainly as user accounts, activity connected to those accounts, and free text you write yourself.

2. Our role, and what this policy covers

Nordic USV AS is the controller, meaning the one who decides how and why personal data is processed, for the personal data we process for our own purposes: creating and securing user accounts, the customer relationship, support, invoicing, operations and security, product analytics, inquiries and quote requests, and the newsletter. This policy covers that processing. It applies in particular to

- users and organization administrators in organizations that use [Kystdata.io](https://kystdata.io)
- contact persons at customers, suppliers and partners
- people who contact us about our services, support or a customer relationship, including through the forms on nordicusv.com
- visitors to nordicusv.com and subscribers to our newsletter

For content the customer and its users put into the platform, such as free text, figure text, uploaded files and contact persons the customer registers, and for the activity log the customer uses to follow up its own users, the customer's organization is the controller and Nordic USV is the processor. That processing is governed by the data processing agreement, which forms part of the terms of service.

We follow the privacy rules that apply, including the General Data Protection Regulation (GDPR) and the Norwegian Personal Data Act.

3. What we process and why

User accounts. To create and manage user accounts we process name and email address. If you have provided a phone number and role, we process those too. We get the data from you or from the organization administrator who invites you. We also keep an activity log of actions in the platform, such as invitations, changes to members and roles, changes to the organization and to missions, and responses to quotes. Organization administrators can see the log for their organization; it is part of the platform. We use the log ourselves for security and fault-finding. Your organization uses it to follow up its own users, and for that use the organization is the controller. We store account data for as long as the account exists. We delete the account when you are no longer a member of any organization in the platform, or when you or your organization ask us to. Activity log entries are kept for as long as the customer relationship lasts, with the user anonymized after the account is deleted.

Support and communication. When you contact us, by email, phone or through the forms on nordicusv.com, we process your name, contact details and the content of your inquiry in order to answer you. We keep inquiries for as long as needed to handle the matter and document the customer relationship, and delete them at the latest when the customer relationship ends, unless bookkeeping rules require longer retention. If an inquiry does not lead to a customer relationship, we delete it when we no longer need it to follow up the matter.

Operations and security. We process technical logs (IP address, timestamps, device and browser information, error details) where necessary to operate the platform and the website securely, find faults and prevent abuse. Technical logs are kept only as long as these purposes require and are then deleted on a rolling basis. When something fails on our servers, the error report goes to PostHog, the same provider as our product analytics below. That happens whether or not you have consented to analytics cookies, because it rests on our legitimate interest in a platform that works, not on consent.

Maps. The maps in the platform load map tiles directly from Mapbox, Kartverket and OpenSeaMap in your browser. Those providers receive your IP address when tiles are loaded, as with any website that shows their maps.

Product analytics. If you consent, we use the analytics tool PostHog to understand how the platform is used and to find faults. The events are then linked to your user account (name and email address). That includes session replay, a reconstruction of what happened on your screen. Everything you type into a form field is masked in your browser before the replay is sent. Without consent we count visits anonymously, without cookies. Read more on the cookie policy page, where you can also change your choice at any time.

Email. We send email that belongs to your use of the platform, such as invitations, notifications and alerts you have set up, via our email provider. We do not send marketing email without a separate consent; see the newsletter in section 4.

4. The website nordicusv.com

Visits. The website sets no cookies and stores nothing in your browser. When you visit it, we process your IP address and technical information about your browser, as described under operations and security in section 3.

Visitor statistics. We count visits and page views with PostHog, without cookies and without storing anything in your browser. Visits are not linked to your name or email address. Errors that occur in your browser on the website are also sent to PostHog so we can fix them.

Contact form and quote requests. The forms send what you fill in to us by email, via our email provider. That is your name, email address and message, and in a quote request also your company, phone number, service and any area you have drawn on the map. We use the information to answer you and, where relevant, give you a quote, and otherwise handle it like any other inquiry (see support and communication in section 3).

Spam protection. The forms use Cloudflare Turnstile to tell people apart from automated bots. When you open a form, Cloudflare receives your IP address and technical information about your browser and device, and uses it to assess whether a person is filling in the form.

Newsletter. If you sign up for the newsletter, we store your name, email address and, if given, your company with our email provider, and send you newsletters about our services and technology. We do this only with your consent. You can unsubscribe at any time with the link in the newsletter or by emailing info@nordicusv.com. We keep the information for as long as you are subscribed. If you unsubscribe, we send no more newsletters and keep the information only to know that you have unsubscribed. If you ask us to, we delete it entirely.

Maps. The maps on the website load map tiles directly from OpenFreeMap and Kartverket in your browser. Those providers receive your IP address when tiles are loaded.

5. AI features

The AI features in Kystdata.io are off by default. Only an organization administrator can turn them on, in the organization settings, and the platform shows what will be shared before they confirm.

When someone in your organization uses an AI feature, we send the content needed to answer the request to our AI provider. That is

- measurement data and metadata about the project, such as parameters, waypoint names and positions, and mission dates
- the figure being worked on, including its title and text
- what the user writes to the assistant

The content can include personal data if the user types it in. We do not send user account data (names, email addresses) or uploaded files.

The model runs at Mistral AI in the EU. It is Mistral's own model, Mistral Large, run on Mistral's own European infrastructure. Under Mistral's terms the content is used only to answer the request and not to train AI models. Mistral may keep the content for up to 30 days for abuse monitoring, inside the EU, and then deletes it. The provider is named in the sub-processor list.

We store your conversations with the assistant so you can continue them later. They are private to you: other users and administrators in your organization cannot read them. A conversation is deleted together with the figure it belongs to, with the project, or with your account.

We make no decisions about you based solely on automated processing that have legal effects or similarly significant effects for you. The AI features produce drafts and suggestions; people make the decisions.

An organization administrator can turn the AI features off again at any time.

Nordic USV also uses AI tools internally, for example to read laboratory documents we receive by email. Those tools are in the sub-processor list. They process documents from our laboratory partners, not your account data.

6. Why we are allowed to process the data (legal basis)

We process personal data because

- we must perform the agreement with your organization and do what is needed to provide the platform (GDPR article 6(1)(b)). As a user you are normally not a party to the agreement yourself, and then we also rely on our legitimate interest in providing the service to your organization (article 6(1)(f))
- you have asked for a quote, and we must do what is needed before a possible agreement (article 6(1)(b)). If you ask for the quote on behalf of a business, we also rely on our legitimate interest in answering that business (article 6(1)(f))
- we have a legitimate interest, meaning a genuine need that outweighs the disadvantage for you, in operating the platform and the website securely, finding faults, preventing abuse, improving them, counting visits to the website and answering inquiries (article 6(1)(f))
- you have consented, for analytics cookies and session replay in the platform and for the newsletter (article 6(1)(a)). You can withdraw consent at any time
- the law requires it, for example the bookkeeping rules (article 6(1)(c))

The AI features rest on the agreement with your organization (article 6(1)(b)) and, for personal data about other people that a user types in, on the customer's instruction as controller under the data processing agreement.

7. Who we share data with

We use sub-processors, meaning companies that process personal data on our behalf and on our instructions, to deliver the platform and the website. The sub-processor list shows what each of them does, where they process the data and when. We keep the list up to date and notify organization administrators at least 30 days before we start using a new sub-processor.

Some sub-processors process personal data outside the EU/EEA. Then we make sure the transfer has a legal basis under GDPR chapter V. For providers in the USA that is the EU-US Data Privacy Framework where the provider is certified, and otherwise the EU's standard contractual clauses (contract terms approved by the EU), with supplementary measures where needed. The basis for each provider, and a copy of the standard contractual clauses we have entered into, are available on request to info@nordicusv.com.

If your organization connects an integration, for example export to OneDrive or Amazon S3, the platform sends data to that provider. That happens under your organization's own agreement with the provider, not ours.

We disclose personal data when the law requires it, for example when a court or a public authority orders us to.

8. Security

We protect the data with technical and organizational measures suited to the risk. Among other things we encrypt data in transit, control access at the database level so that each organization only sees its own data, log activity, and keep system keys and passwords secure. Only the people at Nordic USV who need it to operate the platform have access to production data.

9. Your rights

You can at any time ask us to

- explain how we process your personal data, and give you a copy of it
- correct errors and complete missing data
- delete your personal data when the conditions in GDPR article 17 are met, for example when we no longer need it
- restrict processing, meaning that we only store the data without using it, when the conditions in article 18 are met
- hand over the data you have given us in a structured, machine-readable format (article 20)

You can also object to processing that rests on legitimate interest. Then we stop, unless we can show compelling grounds that outweigh your interests and rights.

To use one of your rights, email info@nordicusv.com. You also have the right to complain to the Norwegian Data Protection Authority: Datatilsynet, Postboks 458 Sentrum, 0105 Oslo.

10. Changes to this policy

We update this policy when needed and publish changes on this page. The version that applies, and from when, is shown at the top. If the changes are material, we notify users in the platform.

This policy is available in Norwegian and English. In case of conflict, the Norwegian version prevails.