

Noro Privacy Policy

8 September 2026

Prior Versions: 1 July 2024

See this document online [here](#)

What We Collect

Noro Website

The Noro corporate website (www.Noro.co), the “Noro Website,” is managed by Shared Space Studios, Inc., a Delaware registered corporation with headquarters in Brooklyn, New York, USA.

When you fill out a form on the Noro Website, we will create a record in our systems including information such as your name, email address, company, role, and phone number. We use this information for marketing purposes.

As a visitor to the Noro Website, you can ask us whether we have a profile and information (such as forms filled out and pages visited) about you and, if so, to view, correct, or delete it. For this, please write to [privacy \(at\) noro \(dot\) co](mailto:privacy@noro.co) and provide your email address so we can search for what information we might have tied to that email address. Please note that for most visitors, we don’t have any such information. Additionally, any e-marketing communication you receive from us contains a link to unsubscribe.

We contract with third-party service providers to host the Noro Website and to provide us with other services related to this website, such as helping us automate our marketing interactions. We require our service providers to agree not to access or use any information or data they may have access to while providing services to Noro other than as specified by us.

None of the data we might collect about visitors of the Noro Website is sold or even shared with any third party.

Noro Portal Service

Noro provides organizations with an immersive videoconferencing and collaboration suite, the “Noro Portal Service.” The Noro Portal Service currently consists of two layers, Presence and Collaboration; a third layer, Intelligence — persistent memory across meetings — is planned but not yet generally available (see “A Note on Our Upcoming Intelligence Layer” below).

The use of the Noro Portal Service doesn’t require any name or other profile information, but we will collect your email address to provide you with some specific features, such as being invited to a connection using the Noro Portal Service, or receiving a link to retrieve a recording of a connection. We do not otherwise know or ask for your name.

If you need to access a protected resource while using the collaboration part of the Noro Portal Service, you might have to authenticate to the repository of that resource, or to the SSO of your organization — but not to Noro. Similarly, if you are the host of a Zoom or Microsoft Teams meeting, you will need to authenticate with Zoom or Microsoft Teams respectively, or with the SSO of your organization, in order to host that meeting via the Noro Portal Service.

Except for some administrative access not available to regular users of the Noro Portal Service, we do not create user profiles. Where an account is created (for example, to receive an invitation), sign-in uses passwordless authentication (a “passkey”) rather than a password. We store the public key associated with your passkey, which — unlike a password — cannot by itself be used by anyone, including Noro, to sign in as you.

Meeting Recordings, Transcripts, and Whiteboard Content

For a Noro-native connection (that is, one not hosted via Microsoft Teams or Zoom integration), a host may choose to record it. Recording is captured with the assistance of Daily.co, a third-party video platform provider, and the resulting recording is then stored on our own infrastructure and made available to the host via a link. We automatically delete a recording seven days after the connection ends.

A transcript of a Noro-native connection may also be generated. Unlike a recording, a transcript is only held for the duration of the connection itself and is automatically and permanently cleared the moment the connection ends — it is not retained afterward.

Where whiteboarding is used during a connection, the whiteboard content is processed with the assistance of TLDraw, a third-party whiteboarding platform provider, for the duration of the connection only, and is automatically cleared when the connection ends.

If your connection is instead hosted via Microsoft Teams or Zoom integration, any recording of that meeting is a feature of, and is created, accessed, and stored entirely by, Microsoft Teams or Zoom — Noro does not access, process, or store any such recording under any circumstance.

Live audio and video during a Noro-native connection is handled by Daily.co, the video platform that powers such connections; Noro is not itself a videoconferencing or WebRTC platform, and our own infrastructure never receives or has access to this live audio or video. Daily.co's access to this content is what allows it, at the host's option, to produce the recording and transcript described above; Noro receives only the resulting recording and transcript, not the underlying live stream.

Artificial Intelligence

The currently available Noro Portal Service uses on-device machine learning, running locally on the portal's own hardware, to recognize when a video stream comes from a room camera versus an individual's device (so that each can be displayed at an appropriate size), and to anonymously track the position of people within a room so that individual participants can be shown separately to remote viewers. This on-device process does not perform facial recognition or any other form of biometric identification, and it does not create or retain any identity that persists beyond the connection in which it operates. No customer data, video, or audio is used to train any machine learning model, by Noro or by any third party.

A Note on Our Upcoming Intelligence Layer

We are developing an Intelligence layer for the Noro Portal Service that will allow meeting content to build into a persistent, organization-specific memory over time, expected to become available in late 2026 or early 2027. When this feature becomes available, the associated meeting-derived content is intended to be stored within infrastructure controlled by the customer organization itself, rather than by Noro. We will update this policy accordingly before that feature is made available.

Subprocessors

In providing the Noro Portal Service, we rely on the following categories of third-party subprocessors: (i) Amazon Web Services (AWS), which hosts our backend infrastructure, including stored recordings and account/operational data; (ii) Daily.co, which provides the underlying video platform for Noro-native connections and, at the host's option, generates recordings and transcripts as described above; and (iii) TLDraw, which processes whiteboard content for the duration of a connection. We require each of these providers to safeguard any information they process on our behalf and to use it only as we direct.

No Tracking of Your Browsing

Noro Website

We use Google Analytics code and some similar tools on the Noro Website to obtain browsing statistics with the purpose of making the website more relevant for our visitors. Browsing statistics are aggregate data (such as number of page views, sessions, percentage of new visitors vs. returning users) that do not provide Noro with any personal data such as your name, IP address, device identifier, or email address. Please see Google Analytics' privacy policy for current details on Google's practices.

Noro does not collect data about your browsing behavior beyond the Noro Website.

Noro Portal Service

There is no tracking of your personal browsing behavior implemented in the Noro Portal Service. Separately, we do collect operational telemetry about the portal hardware itself — such as software version, connectivity quality, and how often and for how long a portal is used — to operate and support the fleet of portals. This telemetry is about the portal hardware and its usage, not about you personally, and is not used to track any individual's browsing.

Security

Noro Website

We implement SSL certificates on the Noro Website so that you can have the guaranty, while browsing on it, that you are on a trusted and legitimate website. We also use these certificates to encrypt (https) the information you enter on the Noro Website by filling out a form. The information you provide and the data that might be gathered from further interactions with the Noro Website is stored under our direction by our Marketing Automation and Customer Relationship Management service providers, who have stated in their privacy policies that they have put in place suitable physical, electronic, and managerial procedures to safeguard and secure this information.

Noro Portal Service

We have policies in place to use appropriate physical, electronic, and managerial procedures to safeguard and secure the data we may collect from the usage of the Noro Portal Service, such as email addresses and recordings. Traffic to and from our own infrastructure is encrypted in transit, and data such as recordings is encrypted at rest; a transcript, being held only for the duration of a connection and never stored afterward (see “Data Retention” below), is secured only for that brief period. As described above, we require our subprocessors to apply comparable safeguards to any data they process on our behalf.

What Data Is Sent Outside the EU and Where

Some of the service providers and subprocessors described in this policy — including those supporting the Noro Website and, for the Noro Portal Service, Amazon Web Services, Daily.co, and TLDraw — may process data outside the European Union. Where we transfer personal data originating in the EU to a country that has not been recognized as providing an adequate level of protection, we put in place an appropriate safeguard, such as the European Commission's Standard Contractual Clauses, before doing so.

Government Requests

Notwithstanding anything to the contrary in this policy, we may preserve or disclose your information if we believe that it is reasonably necessary to comply with a law, regulation, or legal request or to protect the safety, property, or rights of Noro or others. However, nothing in this policy is intended to limit any legal defenses or objections that you may have to a third party or government request to disclose your information.

Data Retention

Noro Website

Given the retention requirements of some regulatory bodies as well as the limited data we receive and the nature of its purpose, we do not have a data deletion policy in place yet.

Noro Portal Service

Recordings of Noro-native connections are automatically deleted seven days after the connection ends. Transcripts and whiteboard content are automatically cleared the moment a connection ends and are not retained afterward. Operational data such as logs, usage telemetry, and account information are retained for the duration of an organization's contract with Noro and are automatically deleted within 90 days of that contract ending. These are our standard retention periods and are not currently customer-configurable; as noted above, this is expected to

change for meeting-derived content once our Intelligence layer becomes available, at which point that content is intended to be retained within the customer organization's own infrastructure instead.

Change of Control

If Noro is ever involved in a bankruptcy, merger, acquisition, reorganization, or sale of assets, your information may be sold or transferred as part of that transaction. The promises in this policy will apply to your information as transferred to the new entity, including your right to delete your information entirely from our databases.

Changes and Contact Info

From time to time, we need to make changes to our Privacy Policy to account for new features or for other reasons. When such changes occur, you are able to track them on our website as well as view the new document on our website. By continuing to visit the Noro Website or use the Noro Portal Service, you are consenting to the revised policy. If you have concerns about our policy, please forward them to [privacy \(at\) noro \(dot\) co](mailto:privacy@noro.co), and we'll try our best to respond promptly.