NovaLink

Published notice — status, accuracy and right to amend. This document is published by the Company in good faith for general information and transparency. It is current only as of its stated date and is provided “as is,” without warranty of completeness or accuracy; it may contain errors or omissions and does not constitute legal, financial, tax, or investment advice, an offer or solicitation, or any guarantee. The Company may revise, correct, update, supplement, or withdraw this document at any time without prior notice, and the version published on the NovaLink Transparency Portal is the controlling current version and supersedes any earlier copy. Where this document conflicts with a signed agreement between you and the Company, or with applicable law, that signed agreement or applicable law prevails. If you believe anything here is inaccurate or out of date, please contact support@novalink.tech so we can review it and, where appropriate, correct it. To the maximum extent permitted by law, the Company accepts no liability for any reliance placed on this document.

Latin America Data Protection Memorandum

Who holds your data, what we can and cannot see, and the law of each country — for participants across Latin America

Document ID: NL-LATAM-01
Version: 1.1 (revised 10 November 2026)
Status: Position memo
Issuing entity: Group-wide policy — adopted by each NovaLink entity listed in the Corporate Structure & Entity Register (NL-ORG-01). Data controllers: Ntech Link Technologies Ltd, Co. No. 2195904 (NovaLink Store and web properties) and Auralink Nova Technology L.L.C, Reg. No. 1607764 (Nx1/Hx1 operating environment and applications). Community account and KYC data is controlled by your Community Operator under its own privacy policy
Applies to: participants, Node Operators and prospective participants resident in Latin America, whichever Community Platform they joined through
The NovaLink entities: Ntech Link Technologies Ltd, Co. No. 2195904 (Store Operator) · Auralink Nova Technology L.L.C, Dubai, Reg. No. 1607764 (Technology Provider) · NodeLink USA, Inc., Delaware, File No. 10606222 (US Distribution)
Effective date: 30 July 2026
Contact: support@novalink.tech

1. The question this memorandum answers

“If I run an Nx1/Hx1 Home Station in my house, will NovaLink — or anyone — take, read, or sell my data?” The short answer is no, and this memorandum explains exactly why, in verifiable terms rather than promises: what the machine can physically see, what it cannot see, what little is retained and for how long, which company holds each category, what the law of your country requires, and how to exercise your rights. It is written for participants in Latin America and reflects the data-protection laws of the region as at July 2026.

One important correction to a common assumption: Latin American countries do not share one data-protection law. Each country has its own statute and its own authority — some very strict and modern (Brazil, and Chile from 1 December 2026), some older, and a few with no

comprehensive law at all. Section 5 sets this out country by country. Where no local law applies, the commitments in this memorandum apply anyway: they are our published standard everywhere.

2. What the Nx1/Hx1 Home Station can see — and what it cannot

The Nx1/Hx1 Home Station — one machine, a single model with a single operating system; “Nx1” and “Hx1” are the same machine, named for the participant's community — is a sealed mini-computer that runs verified third-party workloads scheduled by the network. Its technical design (set out in the Technical Security Whitepaper, NL-SEC-01, and Network Architecture & Workload Isolation, NL-ARCH-01) means the following statements are architecture, not policy:

- It cannot see the other devices in your home. Workloads run in an isolated runtime with no route to your local network, the machine's home-network interface sits in its own separate network namespace, and a default-deny firewall on the device protects it. The separation is built into the machine, so your phones, laptops, cameras and smart devices stay out of its reach without any change to your router (NL-ARCH-01, NL-SEC-01).
- It cannot read your browsing, your messages, or your files. Your personal internet use does not pass through the machine — it is a separate device, not a router or gateway. One exception that you choose, stated plainly rather than left to be found: the machine can host an optional WireGuard VPN for the owner's own household (five subscriptions in total). If you choose to switch it on, that VPN traffic does pass through the machine — because that is what a VPN is — and it remains yours: it is off by default, workloads run in a separate isolated environment and cannot see it, and its content is not logged (NL-ARCH-01, NL-LOGS-01).
- Workload content is never stored. The content of workload traffic is discarded in flight and is not retained — see the Data Minimisation & Retention Policy (NL-LOGS-01).
- It has no microphone and no camera.

What the machine does send to the network is limited operational telemetry: its serial number, uptime, aggregate bandwidth counters, its public IP address, hardware utilisation and software version — retained for 90 days and then deleted. Workload session metadata (which workload ran, when, and how many bytes — never the content) is retained for 180 days. That is the complete list; it is published in NL-LOGS-01 and nothing else is collected from the machine. As NL-LOGS-01 itself states, the no-content-logging position has not yet been independently verified; the first independent assurance review is targeted for 2027 — we say this here so that no reviewer has to discover it.

A useful perspective from the industry we exist to replace: for years, some smart TVs, set-top boxes, free apps and even connected home appliances have shipped with embedded software that silently relays third-party traffic through the household's connection — the “residential

proxy" industry, operating without meaningful consent from the family whose internet it uses. Note carefully what even those schemes could not do: relaying traffic through a connection does not open access to the household's files, messages, photos or browsing — carrying traffic and seeing personal data are physically different things. The Nx1/Hx1 Home Station performs the same category of work with the opposite ethics — your explicit, informed agreement, identified participants, published limits and hardware isolation — and with that same physical boundary: it carries verified workload traffic, and it has no access to your personal data.

3. Ten commitments, in plain words

- We do not sell personal data. To anyone. Ever.
- We do not read the content of anyone's traffic — yours or the workloads'. Content is discarded in flight and cannot be recovered afterwards.
- We collect the minimum the network needs to run, publish the complete list, and delete it on the published schedule (NL-LOGS-01).
- Your identity documents (KYC) are held by your Community Operator under its own privacy policy — not by the technology provider, and never on the machine.
- The machine cannot see your home network, and we recommend a network configuration that makes that physically impossible.
- We do not profile you, advertise to you based on your data, or share data with data brokers.
- Any government or police request for data is handled under a published procedure with defined limits (Law Enforcement Request Policy, NL-LE-01) — and content that was never retained cannot be handed over, because it does not exist.
- You can ask what we hold about you, correct it, or ask for deletion at any time: support@novalink.tech.
- Cross-border transfers use recognised safeguards (contractual clauses aligned to the strictest applicable regime).
- If we ever change any of this, the change is published on the Transparency Portal before it takes effect.

4. Who holds which data

Data	Held by	Where governed	Retention
Community account, KYC identity documents, USDN ledger	Your Community Operator (the entity you contracted with on your community platform)	Your Community Operator's privacy policy and agreements	5 years (AML record-keeping)
NovaLink Store purchase records (name, delivery address,	Ntech Link Technologies Ltd (Store Operator)	Privacy & Cookies Policy (this portal)	As required for warranty, tax and consumer law

order)			
Device telemetry from the Nx1/Hx1 Home Station	Auralink Nova Technology L.L.C (Technology Provider)	Data Minimisation & Retention Policy (NL-LOGS-01)	90 days rolling
Workload session metadata (no content)	Auralink Nova Technology L.L.C	NL-LOGS-01	180 days rolling
Workload traffic content	Nobody — discarded in flight, never retained	NL-LOGS-01	Not retained

5. The law of your country — a register

Data-protection law in Latin America is national, not regional. The table below states, for each country, the main statute and supervisory authority as at July 2026. Where our practices are described in this memorandum, they are designed to meet the strictest of these regimes, so participants in every listed country receive the same standard.

Country	Main law	Authority	Notes
Brazil	Lei Geral de Proteção de Dados — LGPD, Law 13.709/2018	ANPD	GDPR-style; standard contractual clauses approved 2024; active enforcement
Mexico	New Federal Law on Protection of Personal Data Held by Private Parties (in force 21 March 2025)	Secretaría de Anticorrupción y Buen Gobierno (replaced INAI)	Privacy notice + ARCO rights retained under the new law
Chile	Law 19.628 (current); Law 21.719 in full force from 1 December 2026	Agencia de Protección de Datos Personales (from Dec 2026)	New GDPR-level regime: 72-hour breach notification, fines to 20,000 UTM / 4% of income
Argentina	Law 25.326 (Personal Data Protection)	AAIP	EU adequacy reconfirmed 2024; GDPR-style reform bills pending
Colombia	Law 1581/2012 and decrees	Superintendencia de Industria y Comercio (SIC)	Active enforcement; habeas data constitutional right; reform under discussion
Peru	Law 29733 and updated regulations	ANPD (Ministry of Justice)	ARCO rights; registration obligations
Ecuador	Organic Law on Personal Data Protection (LOPDP, 2021)	Superintendencia de Protección de Datos	GDPR-influenced; sanctions regime in force
Uruguay	Law 18.331	URCDP	EU adequacy reconfirmed 2024; data protection recognised as a human right
Paraguay	Law 7593/2025 (comprehensive personal data protection)	Authority per the new law	First comprehensive regime, replacing credit-data-only Law 6534/20
Panama	Law 81/2019	ANTAI	Consent-based regime

Costa Rica	Law 8968	PRODHAB	Registration and consent obligations
Dominican Republic	Law 172-13	Sectoral supervision	Consent-based; reform under discussion
Bolivia	No comprehensive statute; constitutional habeas data (Art. 130)	—	Our published commitments apply as contractual standard
Venezuela	No comprehensive statute; constitutional protections (Arts. 28 and 60, including habeas data)	—	Our published commitments apply as contractual standard

Other countries of the region (Guatemala, Honduras, El Salvador, Nicaragua, Cuba, Haiti) currently rely on constitutional or sectoral protections rather than a comprehensive statute; the commitments in this memorandum apply there as our contractual standard.

6. Your rights and how to use them

Every comprehensive law in the region gives you a core set of rights, generally known as ARCO rights — Access (see the data held about you), Rectification (correct it), Cancellation (delete it), and Opposition (object to a use). Brazil, Chile (from December 2026) and Ecuador add GDPR-style rights such as portability. To exercise any of these against the NovaLink entities, write to support@novalink.tech with the subject “Privacy — [your country]”. We respond within the timeframe your national law requires, and if you are not satisfied you may complain to the authority listed in Section 5 for your country. For community account and KYC data, address your request to your Community Operator, which is the controller of that data under its own privacy policy.

Security incidents: if a personal-data breach affects you, we notify the competent authority and the affected participants in line with the strictest applicable regime — including the 72-hour notification standard that Chile's Law 21.719 makes binding from December 2026 and the ANPD notification rules under Brazil's LGPD — regardless of which country you are in.

7. Cross-border transfers

Data processed by the NovaLink entities may be transferred between the jurisdictions in which the entities operate. Transfers are protected by contractual safeguards aligned to the strictest applicable regime (including the standard contractual clauses recognised under the GDPR and Brazil's LGPD). Argentina and Uruguay hold European Union adequacy decisions, reconfirmed in 2024; for the other countries of the region, the contractual safeguards apply. Details are in the Privacy & Cookies Policy and the GDPR Addendum (NL-GDPR-01).

8. Honest status of this memorandum

This is a position memorandum, not a compliance certificate. It accurately describes our architecture, our retention practice and our published commitments, and it summarises national laws in good faith as at July 2026; it has not yet been reviewed by qualified local counsel in each

listed country, and laws change. It must not be circulated as evidence of completed compliance with any country's law. Country-by-country counsel review is on the compliance roadmap (NL-ROAD-01).

9. Contact

All privacy questions and requests: support@novalink.tech — subject “Privacy — [your country]”. Spanish- and Portuguese-language requests are welcome.