Data processing agreement

The agreement between the customer company (data controller) and AREAINFO SAS (data processor) on the personal data that Friolink processes on the customer's behalf. Business customers can sign it: download the PDF, fill it in and send it to info@friolink.com.

Effective October 28, 2026

This is a translation for information purposes. The Spanish version is the reference text.

1. Parties

Data controller ("the Customer"): the company that signs up for Friolink, identified in the signature section or in the commercial contract.

Data processor ("AREAINFO"): AREAINFO SAS, RUT 218998030010, with its address at Av. Italia 4663, apto. 103, Montevideo, Uruguay, represented by Rafael Mauricio Favaro Eula. Contact: info@friolink.com.

This agreement forms part of the Terms and conditions of service and of the commercial contract, if there is one. If they conflict on personal data matters, this agreement prevails.

2. Purpose

AREAINFO processes personal data on behalf of the Customer only to provide the Friolink cold chain monitoring service: recording readings, sending alarm alerts, keeping handling, signature and audit records, generating reports and providing support. The details are in Annex I.

This agreement is governed by Uruguay's Law 18,331 (in particular its articles 10, 11 and 30) and its regulations. When the Customer is in Argentina or Brazil, clause 13 also applies.

3. The Customer's instructions

AREAINFO processes the data only according to the Customer's documented instructions. These instructions are this agreement, the contract and the configuration the Customer sets up on the platform (users, contacts, alert channels, reading retention, integrations).

AREAINFO does not use the data for its own purposes or disclose it to third parties, except to the sub-processors in clause 6 or when a law requires it; in that case it notifies the Customer first, if the law allows.

If an instruction appears to be unlawful, AREAINFO informs the Customer and may suspend carrying it out until it is clarified.

The Customer is responsible for having a legal basis for the data it enters and for informing the people concerned.

4. Confidentiality

AREAINFO ensures that the people authorized to process the data are bound by secrecy (Law 18,331, art. 11), that they access only what is necessary for their work and that this obligation continues after their relationship with AREAINFO ends.

5. Security

AREAINFO applies technical and organizational measures appropriate to the risk to protect the data against loss, unauthorized access, alteration or disclosure (Law 18,331, art. 10). The main ones are in Annex II.

AREAINFO may update those measures as long as they do not lower the level of protection.

6. Sub-processors

The Customer authorizes AREAINFO to use the sub-processors in Annex III to provide the service.

AREAINFO notifies the Customer by email 30 days in advance before adding or changing a sub-processor. The Customer may object on reasonable data protection grounds; if no solution is found, it can cancel the affected service without penalty.

AREAINFO chooses sub-processors that offer sufficient guarantees, imposes on them by contract data protection obligations equivalent to those in this agreement and is liable to the Customer for their compliance.

7. International transfers

The data is stored on AREAINFO servers in Uruguay. Some sub-processors process data in other countries (Annex III). Those transfers are made only in the cases allowed by article 23 of Law 18,331 and with the contractual safeguards each sub-processor offers. By accepting this agreement, the Customer instructs AREAINFO to make the transfers necessary to provide the service.

8. Help with data subjects' rights

If a person asks AREAINFO for access to, or rectification, updating, inclusion or erasure of, data it processes on behalf of the Customer, AREAINFO forwards the request to the Customer within 2 business days and does not answer it on its own, unless the Customer asks it to.

AREAINFO helps the Customer respond, with the platform's features (editable profile, account deletion, exports) or with any information needed.

9. Security incidents

If AREAINFO becomes aware of a security incident affecting the Customer's personal data, it notifies the Customer without delay and at the latest within 48 hours of becoming aware of it, so the Customer can meet its own notification obligations to the URCDP and the affected people (Law 19,670, art. 38, and its regulations).

The notification includes, as far as they are known: what happened, what data and how many people may be affected, the likely consequences, the measures taken or proposed and a contact. AREAINFO adds information as the investigation progresses and documents the incident.

10. Return and deletion at the end

When the service ends, AREAINFO delivers to the Customer, on request, a full export of its data in open formats (CSV and PDF) within 15 business days.

It then keeps the data for 90 days to allow recovery and then deletes or anonymizes it, including in backups when they are renewed, except what a law requires it to keep. At the Customer's request, AREAINFO confirms the deletion in writing.

11. Information and audit

AREAINFO makes available to the Customer the information needed to show that it complies with this agreement: security documentation, answers to security questionnaires and the change log.

The Customer may carry out, or have an auditor bound by confidentiality carry out, one audit per year, with 30 days' notice, during business hours and without affecting the service or other customers' data. Each party bears its own costs. An additional audit may be carried out after a serious incident.

12. Liability and term

Each party is liable for its own breaches of this agreement and of the law, within the limits of the Terms and conditions of service, to the extent permitted by law.

This agreement remains in effect while AREAINFO processes data on behalf of the Customer and until the return and deletion are complete.

13. Argentina and Brazil

Argentina: when the Customer is in Argentina, AREAINFO acts as a provider of data processing services on behalf of third parties under article 25 of Law 25,326: it uses the data only for what this agreement provides, does not transfer it to others and destroys it when the service ends, unless the Customer expressly authorizes it to keep it. The security measures are those in Annex II.

Brazil: when the LGPD (Law 13,709/2018) applies, the Customer is the controller and AREAINFO is the processor (operadora, art. 39); international transfers are made with the safeguards of art. 33 and incidents are notified to the Customer within the period in clause 9 so it can notify the ANPD and the data subjects.

14. Governing law and jurisdiction

This agreement is governed by the laws of the Oriental Republic of Uruguay and any dispute is submitted to the courts of the city of Montevideo, unless a mandatory rule provides otherwise.

Annex I. Details of the processing

Aspect	Details
Data subjects	The Customer's staff and technicians or third parties the Customer designates (users, on-call staff, supervisors, refrigeration technicians, anyone who handles an alarm from a device's QR code).
Data	Name, username, email, phone, Telegram or WhatsApp username, role, on-call shifts, assigned sites, alert preferences; log of alerts sent; alarm handling (cause, action, comment); electronic signatures (name, meaning, date, time and IP); name and ID document of whoever handles an alarm from the QR code; audit log of changes with IP; sessions and sign-ins. In addition, device readings and alarms and their location, which are not personal data but are protected in the same way.
Sensitive data	Not processed.
Operations	Collection, recording, storage, consultation, sending alerts, generating reports, export, backup, anonymization and deletion.
Purpose	Providing the cold chain monitoring service, the alerts and the traceability records the Customer needs.
Duration	For as long as the service lasts, with the retention periods in the Privacy policy: readings 5 years by default (configurable from 2 to 10), handled alarms and compliance and audit records 7 years; after cancellation, 90 days.
Location	AREAINFO servers in Montevideo, Uruguay (two sites), and the sub-processors in Annex III.

Annex II. Security measures

- Encryption in transit: HTTPS with TLS 1.2 or higher, HSTS; devices connect over MQTT with TLS, with their own username and password per device and permissions limited to their own data.
- Network: the servers do not expose the web port to the internet; access goes through Cloudflare's tunnel and web application firewall. Administration is done only over the internal network or VPN.
- Access: passwords only as a hash; lockout after 5 failed attempts; two-step verification; email alert for sign-ins from new devices; sessions visible and revocable; web session in an HttpOnly, Secure and SameSite=Strict cookie.
- Permissions: roles per module and scope per site; one customer never sees another's data; periodic review of API routes.
- Integrity: readings that the application can only append, with a daily seal chained with hashes; append-only compliance and audit records; electronic signatures that ask for the password again.
- Availability: daily backups, live replication to a second site in Uruguay and service monitoring every minute.
- Secrets: kept out of the code, with restricted permissions; automatic scanning for keys on every code change.
- Staff: minimum necessary access and a confidentiality obligation.
- Incidents: response, logging and notification procedure according to clause 9.

Annex III. Sub-processors

Sub-processor	Service	Country
Cloudflare, Inc.	Network, protection and access tunnel	United States and global network
Google LLC	Email (Google Workspace), notifications (Firebase Cloud Messaging) and sign-in with Google, if turned on	United States and others
Apple Inc.	Notifications on iPhone and iPad (APNs)	United States
Telegram	Telegram alerts, if turned on	United Arab Emirates and others
Meta Platforms	WhatsApp alerts, when turned on	United States and others
Functional Software, Inc. (Sentry)	Technical error logging	United States
Anthropic PBC	AI-assisted analysis of device data (no account data)	United States
Microsoft Corporation	Sign-in with Microsoft, if turned on	United States
OpenStreetMap Foundation and Esri	Maps and address search	United Kingdom and United States

In addition, the services the Customer itself connects (for example, its monitoring center or a webhook) receive alert data on the Customer's instructions and are not sub-processors of AREAINFO.

Signatures

For the Customer (data controller)

Company name

RUT or tax ID

Name and title of signatory

Signature

Date

For AREAINFO SAS (data processor)

AREAINFO SAS · RUT 218998030010

Rafael Mauricio Favaro Eula, legal representative

Signature

Date