DataPrime

Cold-chain monitoring platform

Conformity Statement

Support for the temperature-control requirements of Good Distribution Practice (GDP)

Issued by DataPrime

Technical document - v1.0

1. Purpose and scope

This document describes the scope, capabilities and technical guarantees of the DataPrime platform regarding the continuous monitoring of temperature conditions of sensitive products throughout the cold chain.

DataPrime is a monitoring tool. Its function is to record, in a continuous, reliable and traceable manner, the temperature conditions (and, where applicable, humidity, light and location) of products, and to raise alerts when readings deviate from the configured thresholds.

Allocation of responsibilities

Overall compliance with Good Distribution Practice (GDP, EU 2013/C 343/01) is the responsibility of the wholesale distributor, the logistics operator or the corresponding authorisation holder. DataPrime does not perform, certify or assume the activity of distribution, storage or physical handling of products.

DataPrime provides the temperature monitoring, recording and alerting layer that supports the customer in demonstrating, before its own audits and inspections, the control of environmental conditions required by the GDP guideline chapter on transport and storage. The interpretation of the data, the response to alerts and regulatory compliance remain with the customer.

2. Functional scope of the monitoring

The platform covers, continuously and automatically, the following aspects of cold-chain control:

- Continuous temperature logging through IoT devices (DataPrime HP6) and associated BLE probes, with a timestamp on every reading.
- Per-device and per-probe configurable thresholds, with automatic alerts when temperature leaves the defined range.
- Local alarms on the device itself (independent of connectivity) and platform alerts, with visual, audible and push notification.
- Location traceability via GPS and, as a fallback, cell-based geolocation (LBS), distinguishing the source of each position.
- Consultable and exportable data history, which constitutes the evidence record for audits.
- Detection of intrusion or opening events through a light sensor (where the hardware includes it).

Expressly outside the scope of DataPrime are the physical handling of products, the thermal qualification of vehicles or chambers, the documentary management of the customer's quality system, and any operational decision arising from the alerts.

3. Technical guarantees of the record

So that monitoring data holds value as evidence, DataPrime implements mechanisms that ensure its integrity and availability:

Guarantee	Implementation
Recording continuity	The device measures at a configurable interval and retains readings even when it loses coverage, re-sending them once the connection is restored.

Guarantee	Implementation
Temporal integrity	Every reading carries a timestamp. Readings taken before network synchronisation are corrected retroactively once the real time is obtained.
Autonomous alarm	The temperature threshold is evaluated on the device itself, persisting through low-power mode, without depending on the cloud.
Traceability	Every alert is recorded with its source (internal device or specific BLE probe), severity and instant, and is kept in the history.

4. Architecture, stability and security of the platform

The reliability of a monitoring system depends on both the hardware and the platform that receives, stores and presents the data. DataPrime is built on a modern architecture and industry-reference tools, selected specifically to ensure availability, security and service continuity.

4.1. Technology base

The web platform relies on a set of widely adopted and maintained technologies:

- Next.js and React as the application framework, with TypeScript for typed code that reduces errors at development time.
- Supabase (managed PostgreSQL) as the database, with backups and high availability managed by the provider.
- Clerk as the authentication and identity-management provider, with current security standards.
- Deployment on cloud infrastructure (Vercel) with global delivery, automatic scaling and managed TLS certificates.
- Device data-ingestion server deployed independently, isolating telemetry reception from the web layer.

4.2. Data security

Access to data is protected across several layers:

- Encryption in transit: all communication with the platform takes place over encrypted connections (HTTPS/TLS).
- Per-organisation isolation: each customer accesses only its own data, through row-level security (RLS) policies enforced in the database itself.
- Role-based access control: sensitive operations are restricted by user role, validated on the server on every request.
- Authentication managed by a specialised provider, centralising the control of credentials and sessions.
- Separation of device ingestion through a shared secret, so that only the authorised server can record telemetry.

4.3. Stability and continuity

To ensure a stable and available service:

- Automatic scaling of the infrastructure under load peaks, without manual intervention.
- Automatic reconnection of real-time data streams after transient network outages.
- Redundancy and backups managed at the database level by the provider.
- Type checking across the whole codebase, preventing a broad class of failures before they reach production.

- Incremental, verified deployments, allowing improvements to be introduced without service interruption.

4.4. Data hosting within the European Union

Customer data and device telemetry are stored in a database physically hosted within the European Union (West EU region, Paris, France). Data remains within the chosen European region, supporting compliance with the data residency requirements of the General Data Protection Regulation (GDPR).

The infrastructure providers used are GDPR-compliant and, where they process data outside the EU, rely on recognised legal data-transfer frameworks (such as the EU-US Data Privacy Framework).

4.5. Security certifications of the providers

The platform is built on infrastructure providers that maintain internationally recognised security certifications, audited by independent third parties:

- Database (Supabase): SOC 2 Type II certified, ISO 27001, GDPR-compliant, with encryption at rest (AES-256) and in transit (TLS).
- Application infrastructure (Vercel): SOC 2 Type 2 attestation (Security, Confidentiality and Availability) and ISO 27001:2022 certification, GDPR-compliant.
- Authentication (Clerk): SOC 2 certified, GDPR-compliant, with regular third-party audits and penetration testing.

These certifications correspond to the infrastructure providers on which DataPrime is built. They do not constitute a certification of DataPrime itself, but reflect that the platform relies on an audited infrastructure foundation compliant with industry security standards.

5. Statement

DataPrime declares that the platform provides the continuous monitoring, traceable recording and alerting capabilities for temperature conditions described in this document, built on an architecture oriented towards stability and security.

These capabilities are designed to support the temperature-control requirements of Good Distribution Practice (GDP). Overall regulatory compliance, the distribution activity and the response to alerts are the sole responsibility of the customer.

DataPrime -
info@primelogger.com - panel.primelogger.com

This document is a technical statement of an informative nature about the capabilities of the tool. It does not constitute an official GDP certificate issued by a competent authority, nor a commercial certification by an accredited body.