Information Notice

according to the EU Data Act

Regulation (EU) 2023/2854 • Full Product Portfolio • Article 3 Pre-Contractual Notice

Data Holder	frient A/S (trading as frient)
Corporate Address	Tangen 27, 8200 Aarhus, Denmark
CVR	30720377
Official Website	www.frient.com
Support & Enquiries	help.frient.com • info@frient.com
Document Version	1.0 — June 2025 — reflects obligations applicable from 12 September 2025

Introduction

This statutory Information Notice provides users, purchasers, and third-party recipients with transparent pre-contractual metadata regarding the full hardware product assortment of frient A/S ("frient A/S"). It is compiled to satisfy the explicit product-data transparency requirements of Article 3 of the EU Data Act (Regulation (EU) 2023/2854), which became applicable on 12 September 2025.

All frient devices communicate exclusively via open-standard Zigbee 3.0 mesh protocols. frient A/S does not operate any mandatory proprietary cloud backend and does not store or remotely process data generated by standalone devices in the field. Data generation is local, ephemeral, and controlled entirely by the consumer through their chosen smart home hub or Zigbee controller.

1. Structural Data Architecture

All frient products transmit data locally over Zigbee 3.0 to a consumer-selected smart home hub or Zigbee coordinator. frient A/S:

- Does not operate a mandatory cloud backend for any product in this portfolio.
- Does not store, log, or remotely access device telemetry from end-user installations.
- Does not hold cryptographic backdoors into Zigbee mesh nodes.
- Does not retain historical data from devices — all data reside in the consumer's hub.

The data holder for any cloud-based data retention or analytics is the smart home hub provider chosen by the consumer (e.g. Homey, Home Assistant, SmartThings). Those providers' own Data Act and privacy notices govern data held in their systems.

2. Per-Product Data Specifications (Article 3(2))

The table below provides the mandatory pre-contractual information per Article 3(2) for every product in the frient portfolio. Columns marked * apply only to specific product variants as noted in the data type column.

Product Group	Product(s)	Data Type & Format	Real-Time Capable?	Frequency / Volume
Safety Sensors	Intelligent Smoke Alarm Intelligent Heat Alarm	Binary alarm flags (IAS Zone state) Ambient temperature (°C) Power status Format: Zigbee ZCL hex arrays	**Yes – on trigger**	Heartbeat: every 5 min Immediate alarm <1 KB/packet No persistent log
Water Detection	Water Leak Detector Water Leak Detector Probe	Binary moisture state (wet/dry) Power status Format: IAS Zone cluster attributes	**Yes – on trigger**	Immediate on detection 5-min heartbeat <512 bytes/event No on-device log
Motion Sensors	Motion Sensor Motion Sensor Pro Motion Sensor 2 Pet	PIR occupancy state (binary) Ambient light level (Lux)* Temperature (°C)* Tamper alert* Format: Zigbee IAS + env. clusters	**Yes – on motion**	Immediate on motion Env. updates: 5–15 min <1 KB/event No on-device history
Entry Sensors	Entry Sensor Pro Entry Sensor 2 Pro	Open/close binary state Temperature (°C) Tamper alert metadata Format: IAS Zone + temp. cluster	**Yes – on trigger**	Immediate on open/close Temp: every 5–10 min <512 bytes/event No on-device log
Vibration Sensor	Vibration Sensor	Vibration/movement binary state Temperature (°C) Tamper alert Format: IAS Zone cluster	**Yes – on trigger**	Immediate vibration Temp: every 5–15 min <512 bytes/event No on-device log
Security & Alarm	Smart Siren Intelligent Keypad	Siren: active/inactive state, alarm mode, battery level Keypad: arm/disarm events, PIN input state, tamper alert	**Yes – on trigger**	Event-driven on activation <512 bytes/event No on-device log

Product Group	Product(s)	Data Type & Format	Real-Time Capable?	Frequency / Volume
		Format: IAS Zone + OnOff clusters		
Smart Plugs	Smart Plug Mini Smart Plug Mini 2 (E/F/G)	Instantaneous power (W) Cumulative energy (kWh) Voltage (V), current (A) Relay state (on/off) Format: Zigbee Simple Metering cluster	**Yes – continuous**	Power delta or every 5 min <2 KB/burst No on-device history
Smart Cables	Smart Cable Smart Cable 2	Instantaneous power (W) Cumulative energy (kWh) Relay state (on/off) Format: Zigbee Simple Metering cluster	**Yes – continuous**	Power delta or every 5 min <2 KB/burst No on-device history
Smart DIN Relay	Smart DIN Relay	Instantaneous power (W) Cumulative energy (kWh) Relay state (on/off) Format: Zigbee Metering + OnOff clusters	**Yes – continuous**	10-sec intervals or power delta <2 KB/burst No on-device history
Electricity Meter Interfaces	Electricity Meter Interface 2, LED Electricity Meter Interface 2, P1 EMI Norwegian HAN	Cumulative energy (kWh) Instantaneous power (W) Multi-phase metrics (V, A, Hz)* Format: Zigbee Metering cluster	**Yes – continuous**	Standard: 10-sec intervals P1/HAN: per meter tick <2 KB/burst No on-device history
Climate Sensors	Air Quality Sensor Smart Humidity Sensor	VOC index (ppb) Air Quality only Relative humidity (% RH) Temperature (°C) Format: Zigbee environmental cluster floats	**Yes – periodic**	Every 2–5 min or on delta <1 KB/payload No persistent flash log
Smart Button	Smart Button	Button press event (single/double/hold) Battery level (%) Format: Zigbee On/Off + power config clusters	**No – event only**	Async on press 12-hr battery report <512 bytes/event Stateless after hub confirm
IO Module	IO Module	Digital input states (binary) Output relay states (binary) Format: Zigbee Binary Input / OnOff clusters	**Yes – on change**	Immediate on state change <512 bytes/event No on-device log

Product Group	Product(s)	Data Type & Format	Real-Time Capable?	Frequency / Volume
Zigbee Range Extender	Zigbee Range Extender	Zigbee router/mesh routing metadata only No user-generated sensor data Format: Zigbee network layer	**No**	Network heartbeat only No user data stored or transmitted

** Lux / temperature sensors are present in Motion Sensor Pro and Motion Sensor 2 Pet but not in the base Motion Sensor. Multi-phase metrics apply to Electricity Meter Interface 2, P1 and EMI Norwegian HAN only.*

All on-device storage is volatile (RAM / transient buffer). No product in this portfolio uses non-volatile flash for user data logs. A factory reset permanently clears all network keys and operational state.

3. Data Access, Retrieval, and Erasure (Article 3(2)(d))

3.1 Real-Time Access

Device metrics can be queried or pulled at any time by pairing the device with a compatible Zigbee transceiver or smart home hub. All Zigbee clusters used are documented open standards (Zigbee Cluster Library, ZCL). No proprietary frient account, subscription, or API key is required to access your data.

3.2 Structured Data Export

To export data into structured formats (CSV, Excel, JSON, InfluxDB, etc.), the consumer must use the database export or API functions available in their chosen hub ecosystem. Examples include Homey Developer Tools, Home Assistant SQLite / InfluxDB integrations, and SmartThings API exports. frient A/S does not provide a proprietary export function because frient A/S does not hold the data.

3.3 Complete Erasure

To permanently erase all data from a frient device:

- Locate the physical reset button or pinhole on the device casing.
- Follow the factory reset sequence in the product installation manual (available at frient.com/manuals).
- This immediately and permanently clears all network keys, routing profiles, pairing tokens, and buffer states.

For erasure of data held in the consumer's smart home hub, the consumer must use that hub provider's erasure or account-deletion functions. frient A/S cannot delete data held in third-party systems on the consumer's behalf.

4. Third-Party Data Sharing — Conditions (Article 5)

Under Article 5 of the Data Act, consumers have the right to instruct frient A/S to share device-generated data with a third-party service provider. Because frient A/S does not hold device telemetry, the consumer exercises this right

directly at their smart home hub layer via hub APIs or local data exports — without requiring authorization from frient A/S.

Where a third-party recipient receives data derived from a frient product, that recipient is bound by the following conditions under the Data Act:

- They may only use the data for the purposes agreed with the user, and not for any other commercial purpose.
- They may not use the data to build a competing product or to assess frient A/S's market position.
- They must not transfer the data to entities designated as 'gatekeepers' under the EU Digital Markets Act (Regulation (EU) 2022/1925).
- They must erase the data when it is no longer needed for the agreed purpose.
- They must respect all trade secret protections covering frient firmware, algorithms, and hardware design (see Section 5).
- They must handle any personal data in compliance with GDPR (Regulation (EU) 2016/679).

Should frient A/S deploy optional cloud platforms in the future, all data-sharing requests will follow FRAND (Fair, Reasonable, and Non-Discriminatory) conditions as required under Article 9 of the Data Act.

frient A/S does not charge fees for facilitating data sharing under the Data Act.

5. Intellectual Property & Trade Secret Safeguards (Article 5(10))

While raw environmental data, energy consumption metrics, alarm state parameters, and all other device-generated operational data are fully available to the user under the Data Act, the following remain strictly classified as frient trade secrets, protected under EU Directive 2016/943:

- Machine code and compiled microcontroller firmware binaries.
- Internal hardware schematics and PCB design layouts.
- Proprietary cryptographic security algorithms and key derivation methods.
- Internal calibration coefficients and signal-processing methods.

Any attempt to reverse-engineer or modify frient device firmware without prior written authorisation from frient A/S is strictly prohibited and may result in immediate termination of hardware warranties and service agreements.

6. Public Sector Data Access — Exceptional Need (Chapter V)

In compliance with Chapter V of the Data Act, frient A/S will cooperate with public sector bodies or EU institutions that demonstrate an exceptional, legally backed need for data access (e.g. severe public safety emergency or critical infrastructure failure).

Because frient A/S does not possess remote access to device telemetry from end-user installations, public authorities seeking device data must direct their formal request to the smart home hub provider used by the relevant end user. To submit a formal public sector enquiry to frient A/S, contact: info@frient.com.

7. Dispute Resolution & Competent Authority (Article 8)

If you believe frient A/S has improperly handled your data access rights, unreasonably delayed a portability request, or failed to provide adequate pre-contractual information, you have a statutory right to file a complaint with the national competent authority in Denmark:

Authority	Danish Business Authority (Erhvervsstyrelsen)
Address	Langelinie Allé 17, 2100 København Ø, Denmark
Email	erst@erst.dk
Website	www.erhvervsstyrelsen.dk

Alternatively, consumers may contact the designated Data Act regulatory authority or data protection authority in their EU Member State of residence.

You may also contact frient A/S directly to resolve a data access concern informally before filing a formal complaint: info@frient.com / help.frient.com.

8. Third-Party Supplier Disclaimer

This Information Notice defines the technical parameters of the standard commercial frient hardware assortment sold directly by frient A/S or through authorized distributors.

If your frient devices were supplied as part of a combined package by a third-party commercial security company, energy utility, care-monitoring service, or other system integrator, please consult that provider's own Data Act Information Notice and contractual terms. The obligations of that provider as the 'seller' under Article 3(2) of the Data Act remain their responsibility. frient A/S can provide this document to any such provider upon request at info@frient.com.

This document is reviewed and updated whenever the product assortment changes or regulatory guidance is updated. The version date on the cover page indicates the most recent review. Onics A/S · frient A/S · CVR 30720377