Dyname IKE / Egoboo — Compliance Commitment on EU Data Act

Version: 1.1
Effective Date: 12 September 2025

Dyname IKE, owner of the brand Egoboo, is committed to respecting and safeguarding your data rights under the **EU Data Act (Regulation (EU) 2023/2854)**. This statement explains how Egoboo complies with the Data Act, how you can exercise your rights, and what protections we provide.

---

1. Introduction

Dyname IKE ("Dyname", "we", "our") owns the Egoboo brand and sells connected products including **tablets, Smartphones, Feature phones, Bluetooth watches, Bluetooth speakers, and Bluetooth headphones** ("Connected Products").

Some Egoboo products may connect to or store data on partner-operated servers. These partners act as data holders alongside Dyname IKE. Regardless of where the data are stored, Dyname IKE ensures that your rights under the EU Data Act are respected, and we provide clear channels for you to exercise these rights.

---

2. Data Holder / Data Holding Entities

- **Primary Entity:** Dyname IKE (Egoboo)
- **Registered Address:** Antonis Tritis 15-17, Pilea – Thessaloniki, 55535, Greece
- **Contact Person:** Georgios Apazidis (Product Manager) — g.apazidis@dyname.eu

In cases where partner companies operate servers or provide cloud services for Egoboo products, those partners also act as data holders. Dyname IKE remains responsible for ensuring your rights under the EU Data Act are respected and enforced.

---

3. Connected Products

Egoboo considers the following products as **"Connected Products"** under Articles 2 & 3 of the Data Act, because they generate or collect data concerning their use or environment and can communicate data via wireless or network connections or companion apps:

- Egoboo Tablets
- Egoboo Smartphones
- Egoboo Featurephones
- Egoboo Bluetooth Watches
- Egoboo Bluetooth Speakers & Headphones

---

4. Product Data: What You Generate, How & When

Product Type	Types of Data Generated	Continuous / Real-time	Storage & Retention	Format / Access / Erasure
Tablets	Device performance logs; app usage data; connectivity (WiFi/Bluetooth); system errors; user settings	Some continuous (performance metrics); app usage may be near real-time	On-device (~30 days); optional cloud sync (up to 24 months)	Export via app/USB (CSV, JSON, XML); user may delete or factory reset
Smartphones	Device performance logs; app usage; connectivity (WiFi/Bluetooth/Cellular); system errors; user settings; sensor data (camera, microphone, accelerometer, etc.); optional health/activity data via apps	Yes, continuous / real-time for performance, connectivity, and sensor streams	On-device (varies by app; ~30 days system logs); cloud services (6–24 months depending on user settings/provider)	Export via system tools or apps (CSV, JSON, XML); full wipe/factory reset clears local data; cloud data removable via account deletion
Feature Phones (non-smart)	Call/SMS metadata (time, number, duration); basic connectivity logs; limited device performance data	Call/SMS metadata in real-time; other logs not continuous	On-device storage (~7–30 days depending on model); network operator retains call/SMS records per telecom regulations	Deletion by clearing logs or factory reset; no standard export (operator may provide billing records)
Bluetooth Watches	Health & activity data (steps, heart rate, sleep); connectivity logs; device status	Yes, continuous / real-time	On-device (7 days); app/cloud storage (12–24 months if enabled)	Export via app (CSV/JSON); reset or erase in app/device
Bluetooth Speakers & Headphones	Connectivity logs (pairing history); device status; firmware version; usage statistics; app settings (if used)	Not continuous; only during use	Local logs (~14 days); app/cloud settings up to 12 months	Reset clears logs; export via app (if available)

---

5. Where and For How Long is Data Stored?

- **On-device:** Most usage data are stored temporarily and are overwritten within 7–30 days.
- **Cloud/app (if you enable sync):** Data may be stored securely on Egoboo or partner servers for up to 12–24 months.
- **Raw sensor data:** In many cases (e.g. heart rate signals), raw data is processed immediately and deleted.
- **Analytics data (if you opt-in):** Anonymous performance and crash data may be stored for up to 24 months to help improve services.

---

6. How You Can Access Your Data

- **Direct access via device/app:** Most data can be viewed or exported through Egoboo device settings or companion apps.

- **Export:** Available in structured, machine-readable formats (CSV, JSON, XML).
- **Support request:** If you cannot export directly, contact us (details below).
- **Deletion:** Data can be erased via factory reset, app tools, or by sending us a request.

---

7. Third-Party Access You Authorize

If you authorize a third party (e.g. a fitness or health platform) to access data from your Egoboo product:

- The third party may submit a request to Dyname IKE.
- Dyname will arrange secure transfer of available data, if technically feasible.
- You can manage and revoke third-party access at any time via Egoboo apps or by contacting support.

---

8. Your Rights under the EU Data Act

You have the right to:

- **Access** the data generated by your Egoboo product.
- **Retrieve/export** the data in machine-readable format (CSV, JSON, XML).
- **Erase/delete** your data.
- **Authorize third-party access** to your data.
- **Withdraw consent** to sharing at any time.
- **File a complaint** with the competent authority under Article 37 in your country of residence, work, or establishment.

To exercise these rights, contact us at:

Email: info@dyname.eu
Address: Antonis Tritis 15-17, Pilea – Thessaloniki, 55535, Greece

---

9. Service Termination / Account Deletion

If you stop using Egoboo products or delete your Egoboo account (where available):

- Your account data and associated product data will be deleted.
- You may lose access to services or third-party integrations linked to your account.
- This action may be irreversible.

---

10. Data Security & Safeguards

We use industry-standard technical and organizational measures to protect your data, including:

- Secure transmission (TLS encryption)

- Encryption at rest for stored data
- Role-based internal access controls
- Audit logs of data access and exports
- Regular security reviews and updates

---

11. Changes & Updates

We may update this statement to reflect changes in law, product features, or policies.
Updates will be published on the official Egoboo website, and customers will be notified where appropriate.