

# EU Data Act – Data Transparency Declaration

**Product:** eufy G50 Hybrid Robot Vacuum

**Manufacturer:** eufy / Anker Innovations Limited

**Product Type:** Smart Robot Vacuum Cleaner (Hybrid – Vacuum & Mop)

This declaration explains what categories of data the device may generate, process, share, and store in accordance with the **EU Data Act**, **GDPR**, and EU transparency requirements.

---

## 1. Categories of Data Collected or Generated

### 1.1 Device & System Technical Data

Data inherently generated by the device:

- Device identifiers (model name, serial number, firmware version)
- Operational and performance logs (status, usage counts, error codes)
- Wi-Fi connection status, signal strength, and network identifiers
- Battery charge status and usage statistics
- Cleaning mode settings and runtime metrics

### 1.2 Mapping & Navigation Data

When navigation features are enabled:

- Home layout maps created during cleaning
- Positioning and path data (robot coordinates and route history)
- Obstacle detection patterns and sensor feedback
- Room segmentation and user-defined no-go zones

Mapping and navigation data are used **only** for robot operation unless the user enables cloud sync.

### 1.3 Usage & Interaction Data

- App usage statistics
- Device feature usage logs (cleaning modes, schedules)
- Timestamped events (start/stop/return-to-dock)
- Interaction logs from app or device controls

### 1.4 App & Account Data (Optional)

When the user pairs the robot with the eufy/Anker app:

- User profile identifiers (name or username, email — if created)
- Device nickname and configuration preferences
- Cleaning schedules and settings stored in app
- Remote control settings and logs

The device itself does **not** collect audio, video, or sensitive biological data.

---

## 2. Purpose of Data Processing

Data generated by the eufy G50 Hybrid is processed only for the following purposes:

### A. Essential Operation

- Automated cleaning using mapping and navigation
- Vacuum and mop coordination based on layout data
- Device scheduling and automatic return to dock
- Battery optimization and route planning

### B. App-Enabled Functionality (Optional)

- Remote control and status monitoring
- Cleaning map display and history
- Custom no-go zones and room settings
- Firmware update initiation

### C. Diagnostics & Improvements (Optional)

- Error log reporting
  - Performance stability insights
- These diagnostic logs are only shared if the user consents via app settings.

No data from the device is used for advertising or profiling unless explicitly permitted.

---

## 3. Who Has Access to the Data

### 3.1 Anker / eufy Services

When cloud or app functions are enabled:

- eufy may access device configuration data
- Anonymized diagnostics (if user consents)
- App-linked preferences and remote control logs

Access is limited to what is necessary for providing features and support.

## 3.2 Third-Party Integrations (Optional)

Only when the user enables integration:

- Smart home platforms (e.g., Amazon Alexa, Google Assistant)  
Data shared with these services is governed by their own privacy policies.

## 3.3 Legal Requirements

Data may be disclosed only if required by law (e.g., valid requests by authorities in accordance with EU law).

eufy/Anker does **not sell personal data**.

---

# 4. Data Storage & Retention

## 4.1 On-Device Storage

- Mapping data and local settings stored on the robot
- Navigation and cleaning history retained until overwritten or deleted

## 4.2 App / Cloud Storage (Optional)

If the user connects the device to the eufy app with cloud features:

- Maps and preferences stored in app or cloud
- Cleaning history and settings retained until user deletion

Local data on the robot persists unless reset or cleared by the user.

---

# 5. Transfers Outside the EU

If cloud and remote features are used, data may be processed or stored outside the EU/EEA.

Such transfers are protected with:

- **Standard Contractual Clauses (SCCs)**
- **Adequacy decisions** where applicable
- Encryption and appropriate safeguards

Without cloud connectivity enabled, no data leaves the EU.

---

## 6. User Rights (GDPR & EU Data Act)

Users have the right to:

- **Access** their data stored on device or cloud services
- **Export** data in a structured, machine-readable format
- **Rectify** inaccurate account or preference data
- **Erase** personal or cloud-stored data
- **Restrict** processing for non-essential functions
- **Withdraw consent** for optional analytics or cloud sync

Requests can be made via:

- eufy/Anker app settings
  - Account privacy dashboards
  - Official customer support channels
- 

## 7. User Controls & Data Management

Users can manage or restrict data processing by:

- Disabling cloud or remote access features
- Turning off optional diagnostics in app settings
- Resetting robot to factory defaults
- Removing linked accounts or app access
- Using app privacy controls

Permissions at mobile OS level (notifications, location) can be revoked at any time.

---

## 8. Security Measures

eufy/Anker implements:

- Secure communication protocols (encrypted Wi-Fi, HTTPS/TLS)
- Signed firmware updates
- Authentication requirements for remote/cloud access
- Access control in app and device interfaces

Unauthorised access is prevented unless the user explicitly enables features.