Tuya Helps Customers Comply with the EU Data Act v1.2

Explanation of Compliance Requirements under the EU Data Act

1. Introduction to the EU Data Act

The EU Data Act was officially published by the European Commission on January 11, 2024, and will take effect on September 12, 2025. The regulation aims to promote the fair flow and sharing of data, unlock its potential value, and ensure data security and privacy.

Key requirements include: manufacturers of connected products and IoT service providers must allow users to access, use, and share the data generated by their devices, and provide the necessary technical and contractual support to ensure data portability and transparency.

2. Scope of Application

The EU Data Act applies to:

- **Connected products**: Such as smart home devices, health monitoring devices, connected vehicles, industrial IoT equipment, wearable devices, etc.
- **Related services**: Referring to digital services that are closely related to the connected product at the time of purchase, lease, or use.

3. Definitions and Roles

- **User:** The end user of the App, who is the owner of the data generated by the device.
- **Data Holder:** means a natural or legal person that has the right or obligation, in accordance with this Regulation, applicable Union law or national legislation adopted in accordance with Union law, to use and make available data, including, where contractually agreed, product data or related service data which it has retrieved or generated during the provision of a related service. In this document, the Customer (OEM/ODM App customers and SDK customers) is the Data Holder.
- **Data Processor:** Tuya, as the customer’s vendor, provides services and processes data under the contract.
- **Data Recipient:** The third party to whom the User requests the data to be shared.

4. Data Generation (Type, Format, Collection Frequency, and Volume)

The data generated by products and services may include product configuration data, usage logs, and

basic product information.

Data Attribute Description:

Data Attribute	Product Data
Data Content	Product configuration and usage logs
Data Format	Collected in JSON format; stored in MySQL tables; exported in XLS format
Collection Frequency	Real-time or event-triggered
Data Volume	Typically 0.01MB–5MB per day; IPC devices about 50MB per day
Continuous Real-Time Generation	Only generated when an event occurs or a status changes

Different products may generate different data types:

Product Type	Data Types (Examples – actual data types can be checked on IoT platform)	Daily Volume (mainly status reporting; may increase with frequent adjustments)
Sockets/Switches	On/off status, countdown, network parameters, connection status, device configuration	~168KB
Lighting Products	On/off status, brightness, color temperature, color, dynamic effects, network parameters, connection status, device configuration	~15KB
Major Appliances (ACs, water heaters, refrigerators, etc.)	Power on/off, volume, operating time, water amount/pressure, fan speed, temperature, humidity, swing angle, energy consumption, connection status, device configuration	~3.75MB
Small Appliances (robot vacuums, humidifiers, air purifiers, etc.)	Speed, cleaning area, consumable life, volume, brightness, PM2.5, temperature, humidity, water level, eCO2, network parameters, connection status, device configuration	~979KB
Sensors	Brightness, distance, noise, color temperature, wind speed, temperature, humidity, pressure, flow rate,	~717KB

	pH, liquid level, position, PM2.5, CO, CO2, formaldehyde, network parameters, connection status, device configuration	
Industrial/Agricultural Sensors (valves, temp/humidity sensors, etc.)	Temperature, humidity, irrigation time, water consumption, network parameters, connection status, device configuration	~4.14MB
IPC Products	Audio/video, images, motion detection events, connection status, device configuration	~50MB (depends on bitrate and reporting frequency)
Health/Wellness Products (wearables, body fat scales, etc.)	Heart rate, steps, sleep, body temperature, blood oxygen, activity trajectory, location, network parameters, connection status, device configuration	~464KB
Mobility Products (e-scooters, e-bikes, etc.)	Speed, brightness, mileage, temperature, network parameters, connection status, device configuration	~521KB

Note: Customers may query exact product data types and definitions via the Tuya IoT platform or by consulting their product supplier: Tuya Developer Platform → Product → Click product name → View Function Definitions.

5. Data Storage and Use

5.1 Data Storage

- Data is mainly stored on remote servers (namely, the Frankfurt data center in Germany).
- Product usage logs (DataPoints) are retained for 7 days by default, after which they are automatically deleted (customers can extend retention by purchasing extended storage).
- Product configuration data is retained until the user unbinds the device or deletes their App account.

5.2 Data Use

- **Customer (Data Holder):** Processes data for contract performance, security, troubleshooting, product improvement (if applicable), and advertising (if applicable).
- **Tuya (Vendor/Processor):** Only fulfills contractual obligations with the Customer and does not access the data for its own purposes.
- **Third-Party Services (if applicable):** Data is shared only with the user's explicit consent.

6. Data Access and Deletion

6.1 Customer App/SDK Upgrade

To enable users to easily access and export device data, Tuya has launched a new feature in the App. Users can view and download device data through an intuitive interface. This feature is available in Tuya's public App and open to OEM customers, and also supported for SDK customers.

- **OEM Customers:** Upgrade App to version ≥6.5.0 to enable data access/export automatically.
- **SDK Customers:** Upgrade SDK to version ≥6.4.0.

API documentation:

- https://developer.tuya.com/en/docs/iot/template-v650-update-instructions?id=Kel0zi0nz9nwx
- https://developer.tuya.com/en/docs/app-development/devicemanage?id=Ka6ki8r2rfiuu#title-14-Export%20device%20information
- https://developer.tuya.com/en/docs/app-development/device?id=Ka5cgmmjr46cp#title-10-Export%20device%20information

6.2 Data Access

In accordance with the EU Data Act, product and service providers are required to ensure that users can access and retrieve product data and related service data.

In Tuya-supported OEM apps, users can view or export data directly via the App, or request export through privacy settings:
App → Me → Settings → Privacy Policy Management → Device Data Export → Select Device → Preview Screen → "Export" → Enter Email.

6.3 Data Deletion

Users can delete data at any time by:

- Unbinding the device in the App and selecting "Delete Data"; or
- Deleting their App account.

7. Data Sharing

7.1 One-Time Sharing

Users can export data via the App and manually provide it to third parties.

7.2 Continuous Sharing

EU users can share device data continuously with third parties via an authorization QR code:

1. Prerequisite**:** The customer (App owner) has enabled the "EU Data Sharing Authorization." For instructions, see "Device Data Sharing."
2. Third party registers at https://platform.tuya.com/cloud and subscribes to cloud services.

3. Third party applies for authorization key and generates an authorization QR code.
4. User scans QR code, logs into App, and selects devices to authorize.
5. User can revoke authorization anytime via App → Me → Device → Account & Security → Cloud Development Projects.

Documentation: https://developer.tuya.com/cn/docs/iot/device_data_sharing_usage?id=Kex4vski8ylak

7.3 Fair Compensation & Restrictions

- **Fair Compensation:** Customers, as Data Holders, must share device data with third parties upon user request. Customers agree that Tuya, as technical provider, may deliver this service on their behalf. Under the EU Data Act, the Data Holder may charge the Data Recipient a reasonable compensation for the costs incurred when sharing device data with a third party.
- **Compensation Mechanism:** Tuya may charge data recipients a reasonable fee for server and network expenses (e.g., API calls, server maintenance).
- **Legal Restrictions:** Data cannot be shared directly with "gatekeepers" as defined by the EU Digital Markets Act (e.g., Google, Apple, Amazon), unless otherwise required by law.

8. Data Holder Identity & Contact Information

Customers, as Data Holders, must disclose their organization name, address, and contact details to users.

9. User Complaint Rights

Customers must inform users that:

1. Users have the right to access, export, and delete their device data.
2. Users may file complaints about data processing with the data protection authority of their country of residence.

10. Trade Secrets

- Customers must assess whether user-accessible data involves trade secrets.
- **Tuya's protective measures:**
    - Only user-generated data is accessible.
    - Algorithms and firmware logic are not disclosed.
    - Exported Excel files contain a confidentiality disclaimer reminding users that data may involve trade secrets, without limiting user rights.

11. Contract Term and Responsibility Allocation

- The contract between the Customer and the end user remains in effect for the duration of the user account.
- Users may terminate the contract at any time by deleting their account.
- Customers, as Data Holders, are responsible for disclosure and user rights; Tuya, as Processor, only provides technical support and bears no direct contractual responsibility toward users.

12. Technical and Security Measures

Tuya implements strict technical and organizational measures across data collection, transmission, storage, access, export, and deletion, to prevent unauthorized access, tampering, or disclosure. These include:

- **Encryption:** TLS 1.2/1.3 for data in transit; AES-256 for data at rest.
- **Access Control:** Role-Based Access Control (RBAC) and least privilege, with two-factor authentication.
- **Integrity Protection:** Signatures/checksums to detect and prevent tampering.
- **Audit & Monitoring:** Real-time monitoring of data access and logs, with regular audits and vulnerability scans.
- **Secure Export & Sharing:** Permission checks before export; encrypted transmission of exported data.
- **Compliance Certifications:** ISO 27001, ISO 27701, SOC 2 Type II, and others.

13. What Customers Need to Do

If you operate in the EU, please:

☑ Upgrade OEM App to ≥6.5.0 / SDK to ≥6.4.0;

☑ Consult your legal or compliance experts to disclose EU Data Act Article 3.2 (user data access rights) before product sales;

☑ Consult your legal or compliance experts to disclose EU Data Act Article 3.3 (user rights and complaint mechanisms) when providing App services;

☑ Assess and disclose the scope of user data involving trade secrets;

☑ Enable “EU Data Sharing Authorization” on the Tuya IoT Platform (see “Device Data Sharing” for guidance).