Tuya Helps Customers Comply with the EU Data Act v1.1

1. Introduction to the EU Data Act

The EU Data Act was officially adopted 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 safeguard data security and privacy.

Its core requirements include that connected product manufacturers and IoT service providers must allow users to access, use, and share the data generated by their devices, and must 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

- **Customer**: Refers to Tuya's OEM/ODM App customers and SDK customers.
- **User**: A regular end user of the App.
- **Data Owner**: The user is the owner of the data generated by their device.
- **Data Holder**: The customer is the data holder and also acts as the data controller.
- **Data Processor**: Tuya is the customer's supplier and processes data on behalf of the customer in accordance with contractual obligations.
- **Data Recipient**: When the end user requests to share data with a third party, that third party is the data recipient.

4. How Tuya Helps Customers Comply with the EU Data Act

To meet the compliance requirements of the EU Data Act, Tuya has introduced a new feature in the App that enables users to conveniently access and export their device data. Users can view and download device-related data through an intuitive interface. This feature has been implemented in Tuya's public App and made available to OEM customers, and is also supported for SDK customers.

- **OEM customers**: Upgrade the App to version 6.5.0 or higher to automatically gain data access and

export capabilities.

- **SDK customers**: Upgrade the SDK to version 6.4.0 or higher.

Relevant API documentation links:

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

5. Tuya's Compliance Support for Customers

5.1. Transparency Information for Product Manufacturers (Article 3.2)

Before selling a product, users must be informed in clear and understandable language:

1). The type, format, and estimated amount of data that a connected product can generate

- Customers can query the data types and formats that a connected product can generate through the Tuya IoT platform: Tuya Developer Platform → Product → Click the product name → View the Details of Function Definitions.
- Format: Typically structured in key-value format.
- Estimated volume: varies by device type, e.g., video uploads ~50MB/day, smart plug only a few KB/day.

2). Whether the connected product can generate data continuously and in real time

- When online, connected products can continuously and in real time generate data.

3). Data Storage and Retention

- Connected products store data on cloud servers.
- Device function point (DataPoint) data is retained for a default of 7 days, which can be extended upon customer request (by purchasing extended storage services).

4). How Users Access, Retrieve, and Delete Data

- Users can access and export their data within the app by going to: App - Me - Settings in the upper right corner - Privacy Policy Management - Device Data Export - Select a device - Data preview - Tap "Export" in the upper right corner - Enter the email address to receive the data.
- Users can delete their data at any time by unbinding the device and selecting "Delete Data."

5.2. Transparency Information for Service Providers (Article 3.3)

Service providers must disclose the following information to users:

1). Nature, volume, frequency of data, user access, and retention period

- Nature of data
  - Device information: device name, device ID, online status, activation time, firmware version, etc.
  - Network configuration information: Wi-Fi details and location permissions, used only for device network setup, not uploaded to the cloud.
  - Device usage logs: sensor data and configuration commands sent from the App to the device. Different types of smart devices report different functional data points — for example, a smart lamp may report brightness and color temperature, while a dehumidifier may report temperature and humidity levels.
- Estimated data volume: varies by device type, e.g., video uploads ~50MB/day, smart plug only a few KB/day.
- Collection frequency: usually real-time or event-triggered (e.g., when switching a smart plug on/off).
- Access and export: users may view or export data via the App interface or request data export through privacy settings.
- Storage and retention: device usage logs are retained for 7 days, then automatically deleted.

2). Data generated during the provision of related services

- Device usage logs include configuration commands sent from the App to the device (i.e., service data) and sensor data reported by the device. Please refer to the above section for details.

3). Purpose of data use by data holders

- Customer (data holder): processes data solely for contract performance, security, troubleshooting, product improvement (if applicable), and advertising (if applicable).
- Tuya (vendor/processor): does not access data for its own purposes.
- Third-party services (if applicable): data sharing occurs only with the user's explicit consent.

4). Identity and contact details of the data holder

- The customer, as the data holder, must disclose their name, address, and contact details in their privacy policy or user agreement.

5). How users may request data sharing with third parties

- One-time sharing: users may export data via the App and manually provide it to third parties.
- Ongoing sharing: users may submit a support ticket or send an email, with the option to withdraw at any time.

6). User complaint rights

- The customer must disclose their supervisory authority in the privacy policy and inform users of their right to lodge complaints.

7). Protection of trade secrets

- Customers must assess whether user-accessible data involves trade secrets.
- Tuya's measures include:
  - Allowing access only to user-generated data.
  - Protecting proprietary information such as algorithms and firmware logic.
  - Adding a confidentiality notice in exported Excel files, reminding users that data may contain trade secrets (without affecting users' right to access, export, or share their data).

8). Contract duration and termination

- The contract remains valid while the user maintains an active account. Users may terminate the contract at any time by deleting their account.

6. Data Sharing Fees and Restrictions

- Business users: A small reasonable fee not exceeding cost may be charged to the data recipient.
- Legal restrictions: Data may not be provided directly to "gatekeepers" designated under the EU Digital Markets Act (e.g., Google, Apple, Amazon), unless otherwise permitted by law.

7. Data Portability and Provider Switching

- Tuya supports data portability and "cloud switching" requirements:Users can export data in a structured format via the App as needed.
- For enterprise customers, we provide contractual support for data migration and service termination processes to ensure a smooth transition between service providers.

8. Technical and Security Measures

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

- Encryption: TLS 1.2/1.3 encryption for data in transit; AES-256 encryption for data at rest.
- Access control: Access is based on role-based access control (RBAC) and the principle of least privilege, with support for two-factor authentication.
- Integrity protection: Use of signatures or checks to detect and prevent data tampering.
- Security audits and monitoring: Real-time monitoring of data access and operation logs, with regular security audits and vulnerability scans.
- Export and sharing security: Access permissions are verified before export, and exported data is transmitted via encrypted channels.
- Compliance certifications: Maintenance of ISO 27001, ISO 27701, SOC 2 Type II, and other

international certifications.