# Tuya Helps Customers Comply with the EU Data Act

## 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/app-development/devicemanage?id=Ka6ki8r2rfiuu#title-14-%E5%AF%BC%E5%87%BA%E8%AE%BE%E5%A4%87%E4%BF%A1%E6%81%AF

https://developer.tuya.com/en/docs/app-development/device?id=Ka5cgmmjr46cp#title-10-%E5%AF%BC%E5%87%BA%E8%AE%BE%E5%A4%87%E4%BF%A1%E6%81%AF

**5. Tuya's Compliance Support for Customers**

**5.1. Transparency Information for Product Manufacturers (Article 3.2)**

According to Article 3(2) of the EU Data Act, product manufacturers must provide users with the following information:

● **the type, format and estimated volume of product data which the connected productis capable of generating**

Customers can check the types and formats of data that connected products can generate via the Tuya IoT Platform:

**Tuya Developer Platform → Product → Click the product name → View the Details of Function Definitions**

The customer's connected products may include various electrical devices, such as smart plugs, lighting products, sensors, IP cameras (IPCs), thermostatic radiator valves (TRVs), Zigbee gateways, and others. These devices collect and generate operational and usage data, which may include sensor readings, device status logs, and user interaction data. This data is typically collected in a key-value structured format, and the estimated volume may vary depending on the device type and usage frequency. For example, a smart plug with IoT support may generate only a few KB of data per day.

● **whether the connected product is capable of generating data continuously and in real-time**

When online, connected products can generate data continuously and in real time (e.g., sensor measurements, smart plug power consumption).

● **whether the connected product is capable of storing data on-device or on a remote server, including, where applicable, the intended duration of retention**

Connected products store data on cloud servers. Device DataPoint (DP) data is retained for 7 days by default and can be extended upon customer request (requires purchasing

extended storage services).

● **how the user may access, retrieve or, where relevant, erase the data, including the technical means to do so, as well as their terms of use and quality of service**

Users can view, retrieve, and export their data in the App by following these steps:

Go to the **Me** page in the App → Tap the **Settings** icon in the top right corner → **Privacy Policy Management** → **Device Data Export** → Select the **device to export** → On the preview page, you can view the device data; to export, tap the export icon in the top right corner of the preview page and enter the email address to receive the exported 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)**

According to Article 3(3) of the EU Data Act, relevant service providers must provide users with the following information:

● **the nature, estimated volume and collection frequency of product data that the prospective data holder is expected to obtain and, where relevant, the arrangements for the user to access or retrieve such data, including the prospective data holder's data storage arrangements and the duration of retention;**

● **Nature of data**

○ Basic information about the smart device: device name, device ID, online status, activation time, firmware version, and upgrade information.

○ Network configuration information: Wi-Fi information and location permissions, used solely for device network configuration and 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 will report different functional data points—for example, a smart light 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 may be around 50 MB/day, while a smart plug may generate only a few KB/day.

○ Collection frequency: Typically real-time or event-triggered (e.g., when a smart plug is switched on or off).

○ Access and export: Users can view or export data through the App interface or request data export via the privacy settings page.

○ Storage and retention: Device usage logs are retained for 7 days and then

automatically deleted.

● the nature and estimated volume of related service data to be generated, as well as the arrangements for the user to access or retrieve such data, including the prospective data holder's data storage arrangements and the duration of retention;

Device usage logs include configuration commands sent to the device via the App (i.e., service data) as well as sensor data reported by the device. Please refer to the previous item for related details.

**● whether the prospective data holder expects to use readily available data itself and the purposes for which those data are to be used, and whether it intends to allow one or more third parties to use the data for purposes agreed upon with the user;**

○ The customer, as the data holder, and Tuya, as the supplier and data processor, do not access customer data for any purposes of Tuya's own. Suggested description:

● We process product and related service data solely for the purposes of contract performance, security, troubleshooting, product improvement (where applicable), and advertising (where applicable).

● We share data with service providers acting as data processors for business purposes.

● If you actively choose to integrate third-party services (e.g., third-party voice services), any data sharing will be based on your consent (where applicable).

**● the identity of the prospective data holder, such as its trading name and the geographical address at which it is established and, where applicable, of other data processing parties;**

The customer, as the data holder, should disclose its name and address in its privacy policy or user agreement.

● the means of communication which make it possible to contact the prospective data holder quickly and communicate with that data holder efficiently;

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

**● how the user can request that the data are shared with a third party and, where applicable, end the data sharing;**

○ **One-time sharing**: Users can export data through the App and manually provide it to the third party.

○ **Continuous sharing**: Users must submit a customer service ticket or send an email,

and may withdraw the request at any time.

**● the user's right to lodge a complaint alleging an infringement of any of the provisions of this Chapter with the competent authority designated pursuant to Article 37;**

The customer should disclose its supervisory authority in its privacy policy and inform users of their right to lodge a complaint.

**● whether a prospective data holder is the holder of trade secrets contained in the data that is accessible from the connected product or generated during the provision of a related service, and, where the prospective data holder is not the trade secret holder, the identity of the trade secret holder ;**

● The customer should assess whether the data accessible to users contains trade secrets. Users can view accessible data via the following path: Tuya Developer Platform → Product → Click the product name → View the Details of Function Definitions.

● Tuya implements technical and organizational measures to protect trade secrets, ensuring that only user-generated data is accessible, while proprietary information such as algorithms and firmware logic remains protected.

● The Excel spreadsheet for exported data contains a confidentiality statement: The data you have exported may contain our trade secrets, including but not limited to device functional data points. Please keep such data confidential. This does not affect your right to access, export, or share the data.

**● the duration of the contract between the user and the prospective data holder, as well as the arrangements for terminating such a contract:**

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**

● **Personal/household users:** Data is provided free of charge.

● **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:** Role-Based Access Control (RBAC) and the principle of least privilege, with user access subject to identity verification (e.g., 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.

● **Compliance certifications:** Maintenance of ISO 27001, ISO 27701, SOC 2 Type II, and other international certifications.

● **Export and sharing security:** Access permissions are verified before export, and exported data is transmitted via encrypted channels.