Tuya wspiera klientów w zgodności z EU Data Act

1. Wprowadzenie do EU Data Act

EU Data Act został oficjalnie przyjęty przez Komisję Europejską 11 stycznia 2024 r. i wejdzie w życie 12 września 2025 r. Celem rozporządzenia jest promowanie sprawiedliwego przepływu i udostępniania danych, odblokowanie ich potencjalnej wartości oraz ochrona bezpieczeństwa i prywatności danych.
Podstawowe wymagania obejmują obowiązek, aby producenci urządzeń podłączonych do sieci i dostawcy usług IoT umożliwili użytkownikom dostęp, wykorzystanie i udostępnianie danych generowanych przez ich urządzenia oraz zapewnili niezbędne wsparcie techniczne i kontraktowe w celu zagwarantowania przenoszalności i przejrzystości danych.

2. Zakres stosowania

- Urządzenia połączone: np. inteligentne urządzenia domowe, urządzenia monitorujące zdrowie, pojazdy połączone, przemysłowy sprzęt IoT, wearables itp.
- Powiązane usługi: usługi cyfrowe ściśle związane z urządzeniem w momencie zakupu, wynajmu lub użytkowania.

3. Definicje i role

- Klient: klienci aplikacji OEM/ODM Tuya oraz klienci SDK.
- Użytkownik: zwykły użytkownik końcowy aplikacji.
- Właściciel danych: użytkownik będący właścicielem danych generowanych przez swoje urządzenie.
- Posiadacz danych: klient, pełniący również rolę administratora danych.
- Podmiot przetwarzający: Tuya, jako dostawca klienta, przetwarzający dane w jego imieniu na podstawie umowy.
- Odbiorca danych: strona trzecia, z którą użytkownik zdecyduje się udostępnić dane.

4. Jak Tuya pomaga klientom w zgodności z EU Data Act

Aby spełnić wymogi rozporządzenia, Tuya wprowadziła w aplikacji nową funkcję, umożliwiającą użytkownikom łatwy dostęp i eksport danych urządzenia. Dane można przeglądać i pobierać przez intuicyjny interfejs. Funkcja ta została wdrożona w publicznej aplikacji Tuya i udostępniona klientom OEM, a także obsługiwana dla klientów SDK.

- Klienci OEM: aktualizacja aplikacji do wersji 6.5.0 lub wyższej automatycznie zapewnia dostęp i eksport danych.
- Klienci SDK: aktualizacja SDK do wersji 6.4.0 lub wyższej.

5. Wsparcie Tuya w zakresie zgodności

5.1. Transparentność dla producentów urządzeń (Art. 3.2)

Zgodnie z artykułem 3(2) EU Data Act, producenci muszą zapewnić użytkownikom m.in. informacje o:

- typie, formacie i szacowanej objętości danych generowanych przez urządzenie;
- ciągłości i czasie rzeczywistym generowania danych;
- przechowywaniu danych na urządzeniu lub serwerze zdalnym, w tym okresie retencji;

- sposobie dostępu, pobierania lub usuwania danych, warunkach korzystania i jakości usług.

5.2. Transparentność dla dostawców usług (Art. 3.3)

Zgodnie z artykułem 3(3) EU Data Act, dostawcy usług muszą informować użytkowników m.in. o:

- charakterze, objętości i częstotliwości zbierania danych oraz zasadach dostępu/eksportu;
- danych usługowych i logach użycia urządzenia, okresie retencji (typowo 7 dni);
- wykorzystaniu danych i ewentualnym udostępnianiu ich stronom trzecim;
- tożsamości i danych kontaktowych posiadacza danych;
- prawie użytkownika do złożenia skargi do organu nadzorczego;
- tajemnicach handlowych i ochronie know-how;
- czasie trwania i zasadach rozwiązania umowy.

6. Opłaty i ograniczenia dotyczące udostępniania danych

- Użytkownicy indywidualni/gospodarstwa domowe: dane bezpłatne.
- Użytkownicy biznesowi: możliwa niewielka opłata nieprzekraczająca kosztów.
- Ograniczenia prawne: brak udostępniania danych „gatekeeperom” (Google, Apple, Amazon), o ile prawo nie stanowi inaczej.

7. Przenoszalność danych i zmiana dostawcy

- Możliwość eksportu danych w ustrukturyzowanym formacie przez aplikację.
- Wsparcie kontraktowe dla klientów biznesowych w zakresie migracji danych i wygaszania usług.

8. Środki techniczne i bezpieczeństwa

- Szyfrowanie: TLS 1.2/1.3 (transmisja), AES-256 (przechowywanie).
- Kontrola dostępu: RBAC, zasada najmniejszych uprawnień, 2FA.
- Ochrona integralności: podpisy i mechanizmy kontrolne.
- Audyty i monitoring: logi dostępu, nadzór w czasie rzeczywistym, skany podatności.
- Certyfikacje: ISO 27001, ISO 27701, SOC 2 Type II.
- Bezpieczeństwo eksportu i udostępniania: weryfikacja uprawnień przed eksportem i szyfrowane kanały.

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

- 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.

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 product is capable of generating;

- whether the connected product is capable of generating data continuously and in real-time;
- whether the connected product is capable of storing data on-device or on a remote server, including, where applicable, the intended duration of retention;
- 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.

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;
- 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;
- 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 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 means of communication which make it possible to contact the prospective data holder quickly and communicate with that data holder efficiently;
- how the user can request that the data are shared with a third party and, where applicable, end the data sharing;
- 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;
- 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 duration of the contract between the user and the prospective data holder, as well as the arrangements for terminating such a contract.

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

- 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.