Informacja o przetwarzaniu danych

Produkty WiFi (wypisane poniżej) firmy LED-POL SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ SP.K. współpracują z popularną aplikacją **TUYA- SMART LIFE, SMART LIVING**.

Lista produktów WiFi firmy LED-POL SPÓŁKA Z O.O. SP.K.:

Indeks	Nazwa indeksu	Ean
ORO31001	ORO E27 A60 WIFI DRIVE 9W RGBW	5902533197392
ORO31002	ORO E27 A65 WIFI DRIVE 15W RGBW	5902533197408
ORO31003	ORO-GU10-WIFI-DRIVE-5,5W-RGBW	5902533197415
ORO31004	ORO STRIP 5050 NWD WIFI DRIVE RGBW SET	5902533197422
ORO31005	ORO-CONTRO-STRIP-WIFI-DRIVE-CCT	5902533197439
ORO31006	ORO-CONTRO-STRIP-WIFI-DRIVE-RGBWW	5902533197446
ORO31007	ORO CERES WIFI DRIVE 18W CCT	5902533197453
ORO31008	ORO-E27-A60-FL-WIFI-DRIVE-CLARO-6,5W-CCT	5902533199426
ORO31009	ORO-E27-ST64-FL-WIFI-DRIVE-CLARO-6,5W-CCT	5902533199433

W celu poinformowania się jak dane są przetwarzane do aplikacji **TUYA**, proszę zapoznać się z dokumentem **Tuya Privacy Policy**:

https://developerapp.tuyaus.com/protocol/1479c8096cc01001?lang=en

Poniżej kopia tekstowa tego dokumentu:

Tuya Privacy Policy

Effective date: March 11, 2024

Die deutsche Version finden Sie hier.

Tuya Smart Inc. and its Affiliates (as hereinafter defined) (“we”, “us”, “our”, or “Tuya”) are committed to protecting your privacy. The Tuya Smart Privacy Policy (this “Policy”) describes our practices in connection with information privacy on Personal Data (as hereinafter defined) we process through your use of our products and services(collectively, the “Services”), for instance the Tuya Smart Mobile Application (the “App”) and its connected Smart Devices.

Before you start using the Services, please carefully read this Policy which details our purposes for collecting and processing your Personal Data, as well as how we use, store, share and transfer your Personal Data. In this Policy you will also find ways to exercise your rights of access, update, delete or protect your Personal Data.

If you are a customer located in the European Economic Area (“EEA”) or the United Kingdom (“UK”), the following corporate affiliate of Tuya may also process your personal data, including for purpose of provision of our products, services and support:

Tuya GmbH, in its role as the Data Controller, with its registered address at: Peter-Müller-Straße 16/16a, 40468 Düsseldorf, Germany.

If you have any question regarding this Policy, please do not hesitate to contact us via:

Tuya Customer Service Department: 1-844-672-5646 or service@tuya.com

Tuya Privacy Office: privacy@tuya.com

You are not obliged to provide to us your Personal Data (as defined below). However, we may be unable to provide you with certain products and/or Services if you decline to provide such data. **If you are a child under the age of 16 (or such other age provided by applicable law in your country/region of residence), please read this agreement and the "Tuya Smart Children's Privacy Statement" with your legal guardian or parent and make sure that you and your guardian or parent have clear understanding about our privacy protection practices.For details, please refer to Tuya Smart Children's Privacy Statement.**

Definitions

In this Policy:
Affiliate means any company, firm or legal entity that: (1) is directly or indirectly controlled by Tuya; or (2) directly or indirectly controls Tuya; or (3) jointly with Tuya, controls the same company; or (4) is, directly or indirectly, under common control of the same company with Tuya. Affiliates shall include, without limitation, Tuya's parent companies, subsidiaries, and such subsidiaries under common control of the same parent company as Tuya.
Personal Data means information generated, collected, recorded and/or stored, electronically or otherwise, that can be used to identify an individual or reflect the activity of an individual, either from that information alone, or from that information and other information we have access to about that individual.
Personal Sensitive Data includes personal biometric information, communication records and contents, health information, transaction information, and precise location information, etc., according to various data protection laws and regulations. When we collect Personal Sensitive Data from you, we will generate an explicit notification for your consent before we collection personal sensitive data about you.
Smart Devices refers to those computing devices produced or manufactured by hardware manufacturers, with human-machine interface and the ability to transmit data that connect wirelessly to a network, including: smart home appliances, smart wearable devices, smart air cleaning devices, etc.

What Personal Data Do We Collect?

In order to provide the Services to you, we will ask you to provide necessary Personal Data that is required to provide those Services. Please note that such Personal Data are necessary for carrying out relevant Services that you may require and you are obliged to provide such Personal Data in order to use our Services. If you do not provide your Personal Data, we may not be able to provide you with the Services.

1) Information You Voluntarily Provide to Us

- **Registered Account Data**: When you register an account with us, we may collect your account name and contact details, such as your **email address, phone number, user name, and login credentials**. During your interaction with the Services, we may further collect your nickname, country code, language preference or time zone information into your account.

If you authorize login to the Services with a third-party account, we will obtain from such third party your **account information (such as portrait, nickname**, region etc.) which may be bound

with your Tuya account for quick login. We will ensure compliance with applicable data protection laws and regulations, as well as agreements, policies or documentations agreed with such third party regarding sharing personal information, in processing your Personal Data.

- **Non-registered Account Data**: If you do not want to provide your account data when you start to use any of the Services, you may use the App without logging in or creating an account, namely the “Try Now” mode, and you may still use certain Services, such as searching and browsing any features on the App by creating a guest ID. When you are using the "Try Now" mode, we will not collect Personal Data related to your account; the data being collected is exclusive to the time of entering the App, operating system of your mobile phone, etc. Collection and use of the Personal Data collected here will be limited for the purposes you have authorized in using the additional functions of the App and/or the Smart Devices. For instance, if you enable the location setting in the "Try Now" mode, the location data will be uploaded for supporting the function. Once you exit from the "Try Now" mode, we will remove your data instantly and permanently.

However, if the Services you request or purchase are based on your account, please go to the registration/login page for guidance.

- Feedback: When using feedback and suggestion features in the Services, we will collect your **email address, mobile phone number and your feedback** content to address your problems and solve device failures on a timely basis.

Information based on additional functions:

In order to offer you with more convenient and higher-quality Services with optimized user experiences, we may collect and use certain information if you consent to use of additional functions in the App. Please note, if you do not provide such information, you may continue to use basic Services of the App and connected Smart Devices, but certain features based on these additional functions may not be available. These additional functions may include:

Additional functions based on location information:

When you enable the location-based functions through permission settings on your mobile device, we will collect and process your location information to enable these functions, such as pairing with your Smart Devices. Also, we may collect information about your: a) real-time and precise location, for instance when you choose to use the automation scenarios for controlling your Smart Devices, or b) non-precise geo-location when you use certain Smart Devices or the Services, such as robot cleaner and weather service.

Based on your consent, when you enable the geo-fence feature, your location information will be generated and shared with Google Maps services. Please note that Google has corresponding data protection measures, which you may refer to Google’s Data Processing and Security Terms for more details. You may disable the collection and use of your location information by managing the device level settings, upon which we will cease to collect and use your location information.

You may opt out of the use of your location information ("My - Setting - Privacy Right Setting - Switch on/off Location Information").

Additional services based on camera:

You may use the camera to scan the code by turning on the camera permission to pair with a Smart Device, take video, etc. Please be aware that even if you have agreed to enable the camera

permission, we will only obtain information when you actively use the camera for scanning codes, video recording, etc.
You may opt-out the using of camera permission: "My - Setting - Privacy Right Setting - Switch on/off Camera".

Additional services for accessing and uploading pictures/videos based on photo albums (picture library/video library):

You can use this function to upload your photos/pictures/videos after turning on the photo album permission, so as to realize functions such as changing the avatar, reporting device usage problems by providing photo proofs, etc. When you use the photos and other functions, we will not recognize this information; but when you report a device usage problem, we may use the photos/pictures you upload to locate your problem.
You may opt-out the using of photo album permission: "My - Setting - Privacy Right Setting - Switch on/off Photo Album".

Additional services related to microphone-based service:

You can use the microphone to send voice information after turning on the microphone permission, such as shooting videos, waking up the voice assistant, etc. For these functions, we will collect your voice information to recognize your command. Please be aware that even if you have agreed to enable the microphone permission, we will only obtain voice information through the microphone when you voluntarily activate the microphone in the App.
You may opt-out the using of microphone permission: "My - Setting - Privacy Right Setting - Switch on/off Microphone".

Additional services based on storage permission (Android):

The purpose is to ensure stable operation of the App by utilizing the storage permission. After you give or indicate the permission to read/write your mobile device’s storage, we will access pictures, files, crash log information and other necessary information from your mobile device’s storage to provide you with functions such as information publications, or recording the crash log information locally.
You may opt-out the using of storage permission: "My - Setting - Privacy Right Setting - Switch on/off Storage".

Additional services based on Notification permission:

The reason why we ask you for the permission is to send you notifications about using the products and services, especially if you have purchased security services and you require an alert or message so that you can capture the real-time status.
You may opt-out the using of App notifications: "My - Message Center - Setting - Switch on/off Notifications".

Additional services based on Alert Window permission：

You may choose to bind a camera in the App and require the App to display the real-time image of the camera in a separate window.
You may opt-out the using of alert window information: "My - Setting - Privacy Right Setting - Switch on/off Alert Window".

Additional services based on Bluetooth permission:

You can enable Bluetooth functions after turning on the permission, including controlling the Smart Devices, acquiring device status, and device network configuration. In these functions, we will communicate with terminal devices via Bluetooth. Please be aware that even if you have agreed to enable the Bluetooth permission, we will only use Bluetooth for communication in these scenarios: display device status on the home page and device panel; perform device control on the home page

and device panel; we will use it on the home page and the add device page, for discovering the devices via distribution network.
You may opt-out the using of Bluetooth via "My - Settings - Privacy Setting - Disable/Enable Bluetooth permission".
Additional services based on HomeKit permission (iOS):
You can enable related functions after enabling HomeKit permissions, including discovering Smart Devices, enabling Smart Device network configuration, controlling Smart Devices, and checking device status. Among these functions, we will process data with the "Home“ App that comes with the iOS system through HomeKit. Please be aware that even if you have agreed to enable the HomeKit permission, we will only use it in these scenarios: on the home page, to discover HomeKit devices, HomeKit device network configuration; in "Settings - HomeKit" for discovering HomeKit devices, HomeKit device network configuration.
You may opt-out the using of HomeKit permission via "My - Settings - Privacy Settings-Turn off/on HomeKit permission".
Additional services based on HealthKit (iOS):
You can proactively enable related functions after enabling HealthKit permission, including statistics on weight, height, running, and swimming. In these functions, we will exchange data with the health-related functionalities that comes with the iOS system through HealthKit. Please be aware that even if you have agreed to enable HealthKit permission, we will only use them in these scenarios: when you use the health-related Smart Device, such as body fat scales, bracelets, watch and consent to use the HealthKit, the data reported by the Smart Device will be transferred to HealthKit.
You may opt-out the using of HealthKit permission via "My - Settings - Privacy Settings - Turn off/on HealthKit permission".
Please note that if you turn on any permission, you authorize us to collect and use relevant personal information to provide you with corresponding Services. Once you turn off any permission, we will take it as a cancellation of the authorization, and we will no longer continue to collect Personal Data based on the corresponding permissions, and the related functions may be terminated. However, your decision to turn off the permission will not affect previous collection and use of information based on your authorization.

2) Information We Collect Automatically

- **Mobile Device Information**: When you interact with our Services, in order to provide and maintain the common operation of our Services, to improve and optimize our Services, and to protect your account security as well, we automatically collect mobile device information, such as mobile device model number, IP address, wireless connection information, the type and version of the operating system, application version number, push notification identifier, log files, and mobile network information. Meanwhile, we will collect your software version number. In order to ensure the security of the operating environment or to provide services, we will collect information about the installed mobile applications and other software you use.

- **Usage Data**: During your interaction with our websites and Services, we automatically collect usage data relating to visits, clicks, downloads, messages sent/received, and other usage of our websites and Services.

- **Log Information**: When you use the App, in order to improve your user experience, the system and exception log may be uploaded, including your IP address, language preference setting, operating system version, date or time of access, so that we can facilitate and accurately identify problems and help you solve them in timely manner.

Please note that one cannot identify a specific individual by using device information or log information alone. However, as these types of information, combined with other information, may be used to identify a specific individual, such information will be treated as Personal Data. Unless we have obtained your consent or unless otherwise provided by data protection laws and regulations, we will aggregate or desensitize such information. Additionally, please refer to section titled “Data Retention” of this Policy for data retention periods of such Personal Data.

3) Smart Devices Related Information:

When you use a Smart Device, we will collect some basic and pre-embedded information of the Smart Device and the information generated during your use of the Smart Device.

- **Basic Information of Smart Devices**: When you connect your Smart Devices with the Services, we may collect basic information about your Smart Devices such as device name, device ID, online status, activation time, firmware version, and upgrade information.
- **Information collected during the process of connecting to a Smart Device**: Based on the type of Smart Device you need to connect, whether the Smart Device is connected via Wi-Fi, via Wi-Fi after establishing a local connection via Bluetooth, via Bluetooth or via Zig-bee, we will collect the Mac address of the smart device.
- **Information Reported by Smart Devices**: Depending on the different Smart Devices you elect to connect with the Services, we may collect different information reported by your Smart Devices. The following information reported by the Smart Device only applies when you use them:
- When you voluntarily use a smart camera (IPC service) and connect to the Tuya platform: When you connect a doorbell camera, a door lock, or a smart surveillance camera through Tuya service to monitor the security of your residence, during the process, the device may capture the images if it recognizes someone or an object is moving around, and then provide you a playback of related surveillance content. At this time, we will automatically encrypt the captured image and save it locally on the device. When you actively choose and successfully purchase cloud storage service, the smart camera will upload the pictures or video files you have taken to the cloud for further storage so that you can review them in the App. We will keep your information based on the cloud storage service you purchase. When you choose to delete the picture in advance in the Tuya App, you can delete it in the message center and if you need to delete a video on the App, the cloud will delete immediately the video files you stored in the cloud service.

Purposes and Legal Basis for Processing Personal Data

The purpose for which we may process information about you are as follows:

- **Provide You with Our Services:** We process your account data, mobile device information, usage data, location information, and Smart Device related information to provide you with

the Services that you have requested. The legal basis for this processing is to perform our contract with you according to our User Agreement.

- **Safety of Our Services:** We process your mobile device information, usage data, location information and Smart Device related information to ensure the functions, and authentication, integrity, security and safety of accounts, activity, products and the Services, to develop and upgrade the Services, to study in-depth the efficiency of our operations and to prevent and trace fraudulent or inappropriate usage. The legal basis for this processing is as necessary for our (or others') legitimate interests.
- **Non-marketing Communication:** We process your Personal Data to send you important information regarding the Services, changes to our terms, conditions, and policies and/or other administrative information. At the same time, we will also send you notifications related to the services you have purchased, such as alert services. You can check the "App Notification" in the App ("Me > Message Center > Setting > Notification Setting") to manage these communications. When you decide not to enable the Notifications function, we will no longer process your information for such purpose. The legal basis for this processing is to perform our contract with you according to our User Agreement.
- **Data Analysis:** In order to analyze the usage of the products we provide and improve your user experience, we may analyze the data you provide us, a) we need to check your problems when you encounter any malfunctions during the usage of the product, under such circumstance, you may not able to opt-out because it is highly related to functionalities and quality of using our product and service, and b) analyze data about how you interface with the product or under particular scenarios so that you can better enjoy the convenience brought by our Services. Your consent is required prior to processing under such circumstances; if you do not agree to data analysis of your data, you can enter the privacy settings of Tuya App ("My > Settings > Privacy Settings > Data Analysis") to opt-out your selection. The legal basis for such processing is based on your consent.
- **Marketing Communication and Personalization:** We may process your account data, usage data, device information to personalize product design and to provide you with services tailored for you, such as recommending and displaying information and advertisements regarding products suited to you, and to invite you to participate in surveys relating to your use of the Services. The legal basis for this processing is your consent. You may give consent to such processing by proactively electing to turn on the Personalization option in the App, and we will not process your Personal Data for such purpose unless your consent has been given to us. If you do not wish for us to continue to process your Personal Data for personalization, you may opt out when you enter the App, or by changing your preferences in "Privacy Settings" ("Me> Settings > Privacy Settings > Personalization") in the App. The legal basis for this processing is your consent. **Please note:** as of the date of latest update of this Policy, we do not use automated decision-making in our Services to process your Personal Data.
- **Legal Compliance**. We disclose information if we are legally required to do so, or if we have a good faith belief that such use is reasonably necessary to:
- comply with a legal obligation, process or request;

- enforce our User Agreement and other agreements, policies, and standards, including investigation of any potential violation thereof;
- protect the rights, property or safety of us, our users, a third party or the public as required or permitted by law; or
- detect, prevent or otherwise address security, fraud or technical issues.

If there is any change in the purposes for processing your Personal Data, we will inform such change to you with a prominent notice on our website of such changes of purposes, and choices you may have regarding your Personal Data.

Who do We Share Personal Data with?

At Tuya, we only share Personal Data in ways that we tell you about. Without your consent, we will not disclose your Personal Data to third-party companies, organizations, or individuals except in the following cases:

- To our third-party service providers who perform certain business-related functions for us, such as website hosting, data analysis, payment and credit card processing, infrastructure provision, IT services, customer support service, e-mail delivery services, and other similar services to enable them to provide services to us.
- To our customers and other business partners who provide you, directly or indirectly, with your Smart Devices, and/or networks and systems through which you access and use our websites and Services.
- To subsidiaries or affiliates within our corporate family for purpose of regular business activities based on our instructions and in compliance with applicable law, this Policy and other appropriate confidentiality and security measures.
- To an affiliate or other third party in the event of any reorganization, merger, sale, joint venture, assignment, transfer or other disposition of all or any portion of our business, assets or stock (including without limitation in connection with any bankruptcy or similar proceedings). In such an event, you will be notified via email and/or a prominent notice on our website of any change in ownership, and choices you may have regarding your Personal Data.
- As we believe in good faith that access to, or use, preservation, or disclosure of the information is reasonably necessary or appropriate to:

(a)Comply with applicable law, regulation, legal process, or lawful governmental request;
(b)Enforce our User Agreement and other agreements, policies, and standards, including investigation of any potential violation thereof;
(c) Protect our operation and business systems;
(d)Protect the rights, property or safety of us, our users, a third party or the public as required or permitted by law; or
(e)Perform risk management, screening and checks for unlawful, fraudulent, deceptive or malicious activities.
Except for the third parties mentioned above, we only disclose your Personal Data to other third parties with your consent.

When you use services provided by third parties, we will make sure that sharing of your Personal Data with such third parties are based on their obtaining your authorization and/or consent, or otherwise in conformity with applicable laws and regulations. We will also make our efforts to manage sharing of any information with these third parties in order to preserve the security of your relevant personal information. For details on such third parties information sharing, please see "List of Third-party Information Sharing". We encourage you to carefully read the privacy policy of any third party with which you interact.
In addition, to ensure operations of the App or to enable certain independent functions, we may embed third-party SDKs in the App. Please note: the types of Personal Data that these third-party SDKs may process are subject to change at any time due to upgrade, updates or policy changes, and you should rely on relevant latest information on the official websites or otherwise made available by such third parties. For details of these SDKs, please see "List of Third-party SDK Services".

Data Transfer

Tuya operates globally, and Personal Data may be transferred, stored and processed outside of the country or region where it was initially collected. Also, the applicable laws in the countries and regions where we operate may differ from the laws applicable to your country of residence (please kindly check Tuya Global Data Center accordingly). Under the Personal Data protection framework and in order to facilitate our operation, we may transfer, store and process your Personal Data in jurisdictions other than where you live.
We protect Personal Data in accordance with this Policy wherever it is processed and take appropriate contractual or other steps to protect it under applicable laws.
The European Commission has determined that certain countries outside of the European Economic Area (EEA), the UK or Switzerland can provide adequate protection of Personal Data. Where Personal Data of users in the EEA, Switzerland, or the UK is being transferred to a recipient located in a country outside the EEA, Switzerland, or the UK which has not been recognized as having an adequate level of data protection, we ensure that the transfer is governed by the European Commission’s standard contractual clauses. You can review the agreement on the basis of approved EU standard contractual clauses per GDPR Art. 46. For more information, see here.
If you would like further details on the safeguards we have in place under the data transfer, you can contact us directly as described in this Policy.

Data Subject Rights

We respect your rights and control over your Personal Data. You may exercise any of the following rights:

- Via the “Me > Settings > Account and Security” or via “Me > FAQ&Feedback” in the Services;
- By emailing us at privacy@tuya.com

You do not have to pay any fee for executing your personal rights. Subject to applicable data protection laws in relevant jurisdictions, your request of personal rights will be fulfilled within 15 business days, or within 30 calendar days due to different response requirement.
If you decide to email us, in your request, please make clear what information you would like to have changed, whether you would like to have your Personal Data deleted from our database or

otherwise let us know what limitations you would like to put on our use of your Personal Data. Please note that we may ask you to verify your identity before taking further action on your request, for security purposes.
You may:

- Request access to the Personal Data that we process about you: "My-Setting-Privacy Settings-Personal Data Export";
- Request that we correct inaccurate or incomplete Personal Data about you: 1) Modify your account number (email address or phone number): "My-Setting-Account and Security-Change your Account"; 2) Modify the nickname and/or time zone: "My-Personal Information";
- Request deletion of Personal Data about you: "My-Setting-Account and Security-Delete Account", when you confirm the deletion of your account, your Personal Data will be deleted accordingly.
- Request restrictions, temporarily or permanently, on our processing of some or all Personal Data about you: Please send over your request through "My-FAQ & Feedback", or send over the email request to privacy@tuya.com;
- Request transfer of Personal Data to you or a third party where we process the data based on your consent or a contract with you, and where our processing is automated: Please send over your request through "My-FAQ & Feedback", or send over the email request to privacy@tuya.com;
- Right of Data Portability: Request to have Personal Data provided to you so that you can provide or “port” them to another provider, by sending the request via email to privacy@tuya.com.

Withdrawal of Consent

You have the right to withdraw or object to our use and processing of your Personal Data, where such use and processing is based on your consent or our legitimate interests. Please kindly check the following instructions detailed in the section below for details:
1)For privacy permissions acquired through device system settings, your consent can be withdrawn by changing device permissions, including location, camera, photo album (picture library/video library), microphone, Bluetooth settings, notification settings and other related functions;
2)You may opt-out the non-marketing communication through “Me > Message Center > Notification Settings” to manage your selection;
3)You may opt-out the data analysis features through “Me > Settings > Privacy Settings”;
4)You may opt-out the Personalization feature through “Me > Settings > Privacy Settings > Personalization”;
5)Unbind the Smart Device through the App, and the information related to the Smart Device will not be collected;
6)By using product with the Try Now mode, and not enable certain location setting for particular smart scene, we will not collect any Personal Data about you;
7)If you previously agreed to associate Tuya account with a third-party service, such as a health platform, please unbind it on the third-party platform.
When you withdraw your consent or authorization, we may not be able to continue to provide you with certain products or services correspondingly. However, your withdrawal of your consent or

authorization will not affect the processing of personal information based on your consent before the withdrawal.
Deletion of the Account: You can find the Delete function through “Me > Settings > Account and Security > Delete Account” (Deactivate Account).
If you have more questions, please do not hesitate to contact privacy@tuya.com.

Security Measures

We use commercially reasonable physical, administrative, and technical safeguards to preserve the integrity and security of your Personal Data. Tuya provides various security strategies to effectively ensure data security of user and device.
As for device access, Tuya proprietary algorithms are employed to ensure data isolation, access authentication, applying for authorization.
As for data communication, communication using security algorithms and transmission encryption protocols and commercial level information encryption transmission based on dynamic keys are supported.
As for data processing, strict data filtering and validation and complete data audit are applied. As for data storage, all confidential information of users will be safely encrypted for storage. If you have reason to believe that your interaction with us is no longer secure (for example, if you feel that the security of any account you might have with us has been compromised), you could immediately notify us of the problem by emailing privacy@tuya.com.

Data Retention

We process your Personal Data for the minimum period necessary for the purposes set out in this Policy, unless there is a specific legal requirement for us to keep the data for a longer retention period. We determine the appropriate retention period based on the amount, nature, and sensitivity of your Personal Data, and after the retention period ends, we will destruct your Personal Data.
In detail, the following factors are considered when determining our retention periods of Personal Data:

- The period of time during which an ongoing relationship with you is retained and Smart Devices and/or our Services are provided to you (also see the User Agreement). For instance, your Personal Data is retained for as long as your account with us remains valid or you keep using the Smart Devices and/or our Services;
- Whether we have a legal obligation to keep your Personal Data; or
- Whether retention is advisable in light of our legal position (such as in regard to the enforcement of our agreements, the resolution of disputes, and applicable statutes of limitations, litigation, or regulatory investigation).

If the legal basis is your consent, we will delete your data immediately after you withdraw your consent.
If the legal basis is our legitimate interest, we will delete your data as quickly as possible if there are no overriding legitimate grounds for processing, but in any case in the event of direct advertising.
Personal Data will no longer be retained when you request to remove your Personal Data or withdraw your consent, and we will accordingly complete the task.

When we are unable to do so for technical reasons, we will ensure that appropriate measures are put in place to prevent any further such use of your Personal Data.

Dispute Resolution

If you have an unresolved privacy or data use concern that we have not addressed satisfactorily, please contact our U.S.-based third-party dispute resolution provider (free of charge) at https://feedback-form.truste.com/watchdog/request.

Children’s Privacy

Protecting the privacy of young children is especially important to us. The Services are not directed to individuals under the age of sixteen (16) (or such other age provided by applicable law in your country/region of residence), and we request that these individuals do not provide any Personal Data to us. We do not knowingly collect Personal Data from any child unless we first obtain permission from that child’s parent or legal guardian. If we become aware that we have collected Personal Data from any child without permission from that child’s parent or legal guardian, we will take steps to remove that information.

Your California Privacy Rights

California Civil Code Section 1798.83 permits users of the Software that are California residents to request certain information regarding our disclosure of Personal Data to third parties for their direct marketing purposes. To make such a request, please contact us in accordance with the "Contact Us" section below. We do not disclose Personal Data to third parties for their direct marketing purposes without your consent. Visit our Statement on California Privacy Notice page for more information.

Changes to this Policy

We may update this Policy to reflect changes to our information practices, at least on an annual basis. If we make any material changes we will notify you by email (send to the e-mail address specified in your account) or by means of a notice in the mobile applications prior to the change becoming effective. We encourage you to periodically review this page for the latest information on our privacy practices.

Contact Us

If you have any questions about our practices or this Policy, please contact us as follows:
Tuya Smart Inc.
Postal Mailing Address: 333 West San Carlos Street Suite 600 San Jose, CA 95110
Email: privacy@tuya.com.
For European Union or United Kingdom data subjects, you have the right to lodge a complaint with a supervisory authority concerning Tuya’s data processing activities. For questions, or to exercise your rights as an EU or UK data subject, please contact our EU/UK Representative here:
Name: Rickert Rechtsanwaltsgesellschaft mbH
Email: art-27-rep-hangzhoutuya@rickert.law
Postal Mailing Address: Colmantstraße 15, 53225 Bonn, Germany

You may contact our Data Protection Officer, Mr. Will Yu, by sending an email to privacy@tuya.com.