General Data Protection Regulation (GDPR) WHITEPAPER

Tuya Inc.

TABLE OF CONTENTS

1. DISCLAIMER

This document is a broad overview of the General Data Protection Regulation 2016/679 (GDPR) issued by the European Parliament and Council of the European Union and took effective on May 25 2018, and a demonstration of how Tuya has been dedicated to fully comply with the GDPR regulation with consultation from TrusrArc, a leader in privacy compliance and data protection in the industry.

Tuya spent great effort in the gap analysis and hard work on the remediation of such gaps during the enforcement of GDPR compliance. In July 2019, Tuya received the finalized GDPR Validation Report issued by TrustArc, which takes immediate effect upon the issuance, with time foregoing we implemented the compliance practices throughout the company, we now maintained the Validation Report in 27th January 2021.

This whitepaper serves as the general introduction of GDPR obligations and evidence of enforcement, therefore the target audience of the whitepaper is exclusive to Tuya Customers and relevant stakeholders for familiarization of Tuya privacy and compliance commitments. The document may be subject to change over time, the information, of course, in this whitepaper does not modify existing contractual arrangements.

Tuya believes strongly in protecting corporate Customers and individual Customers' personal data, and understands that being fully compliant with the Data Protection Legislation and its related regulations is critical to help our corporate Customers preserve the trust and confidence of your Customers. This whitepaper presents Tuya's approach to GDPR preparation and compliance. For clarity, this whitepaper may adjust from time to time as Tuya strictly adheres to the Data Protection Legislation ('Legislation'), as such Legislation might be amended, modified, extended, re-enacted, consolidated or replaced as time goes by.

2. TERMS

In this whitepaper, some of particular definitions shall be given prior attention as clearly defined in the GDPR and will appear in the document, the terms listed below and definitions, i.e. 'the authority', 'recipients', 'third party' shall have the same meaning as in GDPR.

"Data Protection Legislation" means, as applicable: (i) EU Directive 95/46/EC (ii) GDPR, and in each case, any related national laws, legislation, rules or regulations, related to privacy and data protection (including legislation made under or in relation to (i) and (ii)). For clarity, a reference to Data Protection Legislation, includes a reference to Data Protection Legislation as amended, modified, extended, re-enacted, consolidated or replaced from time to time.

"controller" means Party that determines how and for what purposes personal data is processed;
"processor" means Party that processes personal data on behalf of the controller;
"data subject" means Individual about whom personal data relates;
"processing" means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;
"personal data" means Any information relating to an identified or identifiable natural person (data subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as: name, identification number, location data and online identifiers (i.e. IP address, cookie ID).

3. APPLICATION SCOPE

3.1. Entity Scope

The GDPR applies to any company that handles the personal data of residents in the European Union (EU) and European Economic Area (EEA). Tuya expands global businesses and operations and EU is one of the key areas Tuya focuses on and directly serves Customers in the region, in the same time Tuya works with partners who conducts business as well, this GDPR applies to each elements of Tuya's business involved, all Tuya Incorporation wholly owned legal entities, subsidiaries, branches as well as registered offices are included:

<table>
<tr><th colspan="3">Tuya Inc.</th></tr>
<tr><th>Asia Pacific</th><th>EU/EEA</th><th>North America</th></tr>
<tr><td>Tuya (HK) Ltd.</td><td rowspan="5">Tuya GmbH.</td><td rowspan="3">Tuya Global Inc.</td></tr>
<tr><td>Hangzhou Tuya Information Technology Co., Ltd.</td></tr>
<tr><td>Hangzhou Tuya Technology Co., Ltd.</td></tr>
<tr><td>Hangzhou Tuya Information Technology Co., Ltd. (Shenzhen Branch)</td><td rowspan="2">Tuya Smart Inc.</td></tr>
<tr><td>TuyaSmart (India) Private Limited.</td></tr>
</table>

3.2. Partners an Customers

However, because Tuya stands firmly in data protection and privacy, it gives all Tuya's partners or Customers the ability to offer their Customers the rights afforded by the GDPR to control their personal data, wherever they live. Separate from the way in which the GDPR applies to Tuya, the regulation also applies to Tuya's Customers who operate in the EU and EEA or colllect personal data when offer products or services, they may rely heavily on the compliance fulfillment in GDPR from Tuya side to ensure the privacy data protection.

However using Tuya alone does not guarantee that a partner or Customer complies with the GDPR, Customers or partners and their Customers must analyze their own business practices, technical and organizational measures to ensure compliance of the GDPR or relevant Data Protection Legislation and ultimately hold the responsibility for compliance with the laws of the jurisdictions in which they operate.

3.3. Validation Scope

The Validation focused on Tuya's IoT Product Line, which includes the following:
IoT platform (data controller);
Tuya Cloud (data controller + data processor);
Tuya Mobile Apps: Tuya Smart App and Smart Life App (data controller)
Other OEM branded App (data processor);
Tuya API/SDK (data processor).

4. CONTROLLER VS. PROCESSOR

4.1. Being a Controller

GDPR carries over the concepts of data controllers and data processors from the Directive 95/46/EC. Similar to the Directive, data controllers and data processors have different obligations under GDPR, and Tuya primarily plays as the role of Data Controller and Data Processor under different business circumstances.

GDPR defines the Controller as the party that determines for what purposes and how personal data is processed. The following checklists set out indicators as to whether a company plays as a controller, a processor. The more boxes tick, the more likely a company will fall within the relevant category.

☐	We decided to collect or process the personal data.
☐	We decided what the purpose or outcome of the processing was to be.
☐	We decided what personal data should be collected.
☐	We decided which individuals to collect personal data about.
☐	We obtain a commercial gain or other benefit from the processing, except for any payment for services from another controller.
☐	We are processing the personal data as a result of a contract between us and the data subject.
☐	We make decisions about the individuals concerned as part of or as a result of the processing.
☐	We have a direct relationship with the data subjects.
☐	We have appointed the processors to process the personal data on our behalf.

When Tuya acts as the data controller, personal data will be directly collected from the users who use the Tuya products and services, in which Tuya can determine the purposes and means of processing of users' personal data as specified in Tuya Privacy

Policy consented by the users in the first place. If any process of the requests handling with personal data made by Tuya is against users' intention, or any misinterpretation of the requests has been made, users can request to opt out of the consent and make complaints to Tuya, prompt corrections will be made.

4.2. Being a Processor

Processor is the party that processes personal data on behalf of the controller.

☐	We are following instructions from Customer else regarding the processing of personal data.
☐	We were given the personal data by a Customer or similar third party.
☐	We do not decide to collect personal data from Customer's individuals.
☐	We do not decide what personal data should be collected from individuals, despite of heavily depending on the service.
☐	We do not decide the lawful basis for the use of that data.
☐	We do not decide what purpose or purposes the data will be used for, i.e. marketing.
☐	We do not decide whether to disclose the data, or to whom.
☐	We do not decide how long to retain the data, but the Customers do.
☐	We are not interested in the end result of the processing.

For client customized Apps or OEM Apps, Tuya is outsourced such data processing function from the data controller. Customers, namely the data controllers, can determine what personal data and how much volume of the data should be accumulated in the App that Tuya supports. Customers, lawfully bound with tuya, shall determine how much data Tuya shall process and how long Tuya shall retain in data carriers. Tuya processes information according to the requirements of Customers, and the processing activities of such information is limited to providing the services that Customers have agreed with Tuya.

4.3. Data Processing Obligations

GDPR outlines 7 data protection principles and it gives Tuya enlightenment on how to conduct data processing activities as the data controller and processor respectively.

1. Personal data must be processed lawfully, fairly, and in a transparent manner in relation to the data subject ("lawfulness, fairness, and transparency").

The Privacy Policy will be brought to users' awareness when users learn about Tuya's products and services, it provides them a communication in a clear and understandable way describing information categories Tuya will collect from the users and what processing activities will be engaged concerning their personal data, as well as how to exercise the individual right in relation to the personal data Tuya collects.

The Privacy Policy may be amended and updated in a timely manner and promptly inform the user of the changes in the latest announcement and notification.

2. Personal data must be collected for specified, explicit, and legitimate purposes and not further processed in a manner incompatible with those purposes ("purpose limitation").

Under the principle of 'purpose limitation', Tuya provides clear clarifications in the Term of Use and the Privacy Policy about the processing activities of the personal data and only process personal data in the way and for the reasons that agreed upon. If additional processing for new purposes are planned in connection with the activity, an updated privacy notice describing those purposes and any additions to the information previously provided will be made available to the individuals.

3. Personal data must be adequate, relevant, and limited to what is necessary to achieve those purposes ("data minimization").

The data minimization principle is pretty straightforward in Privacy Policy and Data Inventory for Processing that Tuya only collects personal information with the minimum necessity that users agreed with and will never collect information that leave for undetermined period time to come.

4. Personal data must be accurate and kept up to date ("accuracy").

It's quite of importance to keep users' data up-to-date not only for the sake of delivering the products and service to the users in a timely fashion, but the multifaceted risks triggered from the inaccurate data can be avoided. Any requests to update or rectify the personal information will be verified and handled correctly, such rectifications will be synchronized to Tuya's database.

For example, Customers who use Tuya Notification SMS to communicate with their end users should make sure that users' contact information are updated and accurate. any changed of users phone number shall be timely reflected because it will be used to contact the user in the near future, otherwise users might miss such notification for the destined purposes.

5. Personal data must be stored no longer than necessary to achieve the purposes for which it was collected ("storage limitation").

Tuya has created the Data Retention Policy and clearly described that Customer information should be retained for a period of time specified in the Retention Policy, unless otherwise agreed. Where appropriately, Customer information shall be returned to the Customer or destroyed, unless required by laws and regulations, and Tuya does not keep any copies.

6. Personal data must be properly secured against accidental loss, destruction, or damage (“integrity and confidentiality”).

Tuya maintains safeguards designed to protect personal information obtained through the Tuya products and services. Three key tenets in Cloud, Communications and Terminal play prominent securty for data protection. Tencent Cloud, Alibaba Cloud, Amazon AWS and MS Azure help Tuya provide Customers with a safe, stable and reliable physical infrastructure. Based on that, Tuya Cloud is equipped a mature network security architecture, including multiple protection mechanisms such as Firewall, WAF, a Unified Defense System, intrusion and prevention detection, etc. to deal with various threats from the outsiders. In the same time, dynamic encryption key and TLS1.2 protocol to encrypt HTTP, MQTT applies to the Communication channel and standardized encryption tools adopted in the Terminals.

For more information about how to secure personal data, please refer to *Tuya Information Security White Paper* in HERE.

7. Data controllers are responsible for and must be able to demonstrate compliance with the above stated principles (“accountability”).

Tuya is accountable for the achievement of the GDPR compliance and the Privacy Management Framework has been documented on the way to fully implement, it includes robust program controls, risk and compliance reporting structures, and assessment and evaluation procedures, etc.

4.4. Subprocessing

When Tuya plays as the Processor, all the data processing activities are instructed from the data controllers, and if Tuya engages another third party to fulfill the contractual obligations set between Customers and Tuya, consent must be obtained from controllers before access to or transmission of any personal data by a subprocessor. The use of subprocessors is limited for the purpose of:

- Store platform/App data;
- Operate the website and other portions of Tuya’s App and Platform;
- Respond to and manage support inquiries.

A list of subprocessors is documented and will be disclosed upon the request from Customer or data subjects.

4.5. Data Inventory for Processing

As a data processor, sources are varied for Tuya to obtain the personal data, for instance, Tuya Cloud, in which data is created through statistical analysis and calculations; OEM banded Apps and data is collected directly from the individuals to whom the data relates;

or through Tuya API/SDK; or data collected passively, for example through online tracking technologies such as cookies and web beacons.

Whether acts as the data controller or processor, adhering to the Article 30 GDPR, Tuya maintains a record of processing activities derived from different business purposes and devices under its responsibility. The disclosure of such data inventory would be only made when there is explicit written request from a particular Customer or user on a lawful and reasonable basis. If any, such records of processing will be made available to the supervisory authority on request.

5. LEGAL BASIS FOR PROCESSING

Personal data cannot be processed except under a recognized legal basis (unless an exemption applies). The GDPR sets out a list of possible legal basis under which personal data may be processed. In most of the cases, Tuya processes personal information and its related information so as to provide products and services have been requested or purchased as described in the Terms of Use, Contract and Service Agreement, etc.

Tuya processes information based on the:

- Consent: Tuya will get the users' clear consent for processing their personal data for a specific purpose which sets out in the Privacy Policy;
- Contract: Tuya will be enabled to process the personal data as agreed in the Contracts or relevant documentations for the defined purposes;
- Legal obligation: The processing of personal data shall comply with the law (not including contractual obligations);

6. INTERNATIONAL TRANSFERS

Under the GDPR, personal data of residents in EU and EEA can only be transferred to recipients outside the EEA if the recipient has adequate protections in place. Tuya launched and possesses a data processing center in Germany. All the EU personal data will securely stored in the server located in Frankfurt, Germany and Amsterdam, Netherlands and with a lawful business purpose, Tuya ensures data international transfer only occurs on the basis of approved EU standard contractual clauses per GDPR Art.46. the contract is published in HERE.

When necessary, Tuya may transfer personal information to subprocessors in other countries (i.e. U.S.) for the processing obligations fulfillment, Tuya will protect that information as described in *Security and Compliance White Paper*, data processing contracts agreed with the Customer, as well as applicable legal requirements ensuring adequate protection for the transfer of personal information to subprocessors.

When the Customer instructs Tuya transfer their data outside of EU/EEA, it is Customer's

obligation to fulfill the standard contract clauses and inform Tuya of such existence.

7. DATA SUBJECTS RIGHTS

The GDPR provides data subjects (in this case, Customers and users) with certain rights over their personal data. Generally speaking, data subject requests must be addressed within one month, unless they are exceptionally complex or numerous.

7.1. Right of Access

Users can access personal data collected by Tuya without additional technical support. If there is inaccessible information, the appropriate personal data shall be provided for the user within 30 days.

The procedure can be navigated in the App: *Me> Setting> Privacy Policy Management> Export Personal Information* and then follow to submit the recipient email address. It can be automatically handled by sending the download link.

Alternatively, users can send a request to privacy@tuya.com specified in the Privacy Policy; when Tuya receives the request, we will confirm the user identity in the form

Note: Under relevant Data Protection Legislation, YOU are entitled as a data subject to obtain from the Company, confirmation as to whether or not we are processing personal data concerning you, as well as to request details about the purposes, categories and disclosures of such data. You can use this form to request information about, and access to any personal data we hold about you. Filling out the form represents you recognizes your information provided are accurate and intention to request on a lawful basis.	
Personal Information details	
Type of Privacy Right	
Email address to confirm the request	
App Name	
Account Name for the App	
Product Device Name	
Device ID: 1) Open App, enter your device control page and click '…' icon on the top right corner; 2) Click 'Device Info', then you can check 'Virtual ID'.	
Any other information that may help us to locate your personal data:	
Specific Details of the Information Requested: -	

Data Subject's Name	
Please return the request to	privacy@tuya.com

The request will be received by privacy office in the first place and will initiate and coordinate to gather technical support and big data team to prepare the data inventory.

The user's personal data will eventually be sent to the e-mail address given by the user within 20 days, in case the user request more information despite the initial ticket.

When Customer's data subject requests to data portability and the Customer confirms Tuya shall assist, the Customer can raise a ticket in the Help Center, by calling the 24*7 service hot-line or filling out online form.

The Customer service personnel will create a work order accordingly and assign it to the corresponding technical director;

The technical director receives the work order and begins processing the request;

The user's personal data will eventually be sent to the e-mail address, or by the link sending in the App within 30 days. The data be provided in a form that is generally used.

7.2. Right to be Forgotten

Data subjects have the right to request their personal data be erased in certain circumstances.

To achieve this, users can proactively delete their accounts by 'Delete Account' in the App. If the user has not logged in to the App for consecutive 7 days after confirming "Delete Account", all the personal data about the user will be physically deleted.

If the user logs in to the App within 7 days even confirmed to deletion, the deletion request will be canceled, as specified in the Privacy Policy.

7.3. Right to Rectify

If there is any inaccuracy, the personal information provided by the user may be manually modified on the App, i.e. the name of the account and the time zone.

For the data collected through the device, such as power and operation logs, the device configuration data, the correction is not allowed.

7.4. Right to Restrict Processing

If one or more of the following conditions apply or will apply to an activity, Tuya will restrict

processing of personal information until the condition is completed or resolved. The restrictions include stopping processing the user's data immediately, keeping the data intended to be deleted, etc.

Conditions:

- The data subject has contested the accuracy of the personal information and Tuya is in the process of verifying the accuracy of the personal information;
- The processing is unlawful and the data subject has requested restriction of the data use rather than erasure of the data;
- Tuya no longer needs the data for the activity or any legitimate further processing as the data has been discarded. However, the data subject may need such data for the establishment, exercise or defense of legal claims;
- The data subject has objected to the data processing and Tuya is in the process of determining whether compelling legitimate grounds for the processing override the interests, rights and freedom of the data subject.

7.5. Right to Object

The individual can object some personal information be processed, such as opt-out of receiving marketing communications according to instructions, withdraw any permission given in the mobile setting, due to these opt-out decision will not impact basic functions provided.

However for the other personal information, the individual may object to the processing of his/her personal information by deleting his/her account.

7.6. Right to Data Portability

There are two ways for a user to send a data portability request:

- Choose *Me> Setting> Privacy Policy Management> Export Personal Information*. After receiving the migration request, Tuya Customer Service Department will communicate with the user to confirm the identity information.
- Send a request to privacy@tuya.com specified in the Privacy Policy. The privacy office will coordinate data preparation.

When Customer's data subject requests to data portability and the Customer confirms Tuya shall assist, the Customer can raise a ticket in the Help Center, by calling the 24*7 service hot-line or filling out online form.

Tuya Customer Service will create a work order accordingly and assign it to the corresponding technical director; Once the technical director receives the work order and begins processing the request;

The user's personal data will eventually be sent to the e-mail address as directed by the Customer within 20 days.

8. DATA PROTECTION & SECURITY

Under the GDPR, controllers and processors are required to implement appropriate technical and organisational measures. In accordance with the requirement, Tuya has implemented many controls and processes identified in the GDPR, including:

- Encryption of personal data;
- Ensuring confidentiality, integrity, availability, and resilience of processing systems;
- Access control mechanism;
- Ensuring availability and access to personal data in the event of a physical or technical incident;
- Performing regular testing, security assessments, and evaluation of technical and organizational security measures

More information regarding data protection & security can be referred to *Security and Compliance White Paper*.

8.1. Data Protection by Design

The Protection Impact Assessment (PIA)

It is verified that Tuya has implemented technical and organizational measures to ensure only personal data that are necessary for each specific purpose of processing are processed, and that is set as default. In order to capture data operation risks before commencement of a business, Tuya enables the PIA/DPIA process in the Compliance Management Center, overseeing the privacy risks. This PIA/DPIA was created as the guiding principle for the business and technology departments on how to identity risks on handling data privacy and providing instructions to assess and remediate the risks to acceptance level.

8.2. Data Retention Policy

According to the Article 30 GDPR, Tuya keeps data in an identifiable form for only as long as necessary for the processing purposes which individuals have been notified and consented to. Tuya determines the appropriate retention period based on the amount, nature, and sensitivity of personal data. Such data will be destructed upon the retention period ends, unless there is a specific legal requirement to keep the data for a longer retention period. Under such circumstance, data are needed for longer periods of time, Tuya has implemented coding, or similar mechanisms to limit the risk to users, and technically Tuya will achieve pseudonimization to protect such personal data.

The Customers shall define their own data retention period and inform Tuya so that we can document and then put into technical implementations.

The data retention under the Tuya solution shall take the following implications into considerations:

1. when the users request to delete the account;
2. When the service contracted with Tuya is upon terminated;
3. When there is no active records happen to a user's account, including its App, product devices, or any voice controllers, etc.

8.3. Data Processing Addendum (DPA)

According to Article 28 GDPR, Tuya prepares a Data Processing Addendum(DPA) for Customer's review and seeking contractual agreement on the data processing activities explicitly described in the Addendum, supporting as explanation of how Tuya will ensure the security and data protection for all trusted processing activities.

Tuya provides advance notice to controllers on the changes of subprocessors and will obtain written consent for such engagement. Tuya also has a resource mechanism handling situations where Customers reject to use subprocessors. In the same time, if a DPA checklist will verify if the vendorship Tuya engages with conducted in a lawful manner - Article 28 GDPR, ensuring all the legal requirements are documented in vendor's DPA, otherwise the DPA shall be revised accordingly.

8.4. Vendor Management

To facilitate Tuya's operation, there is an engagement of subprocessors by transferring certain type(s) of personal data for further processing. Tuya generated the Vendor Risk Management process by evaluating evaluating and downgrading the privacy and security practices of subprocessors to ensure that they have effective technical and organizational safeguards and controls in place. The assessment will be provided before the vendor on-boarding. The assessment will be recorded in Tuya Compliance Management Center for annual check-back. After such assessment and remediation, Tuya uses DPA (designed for Tuya and its subprocessors) to make sure GDPR required contractual obligations have been written down between parties.

8.5. Data Breach Notifications

The GDPR introduces a duty on all organisations to report personal data breach to the relevant supervisory authority. At the minimum requirement, personal data breach, if any, must report within 72 hours of becoming aware of such breach. In the same time, a notification shall be informed to the relevant Customer and its users about the risks, without undue delay, if such incident would potentially and adversely affecting their rights.

Hence, Tuya generated and refined the Incident and Data Breach Response Plan, as a robust breach detection, investigation and internal reporting procedure to tackle with it.

9. ACCOUNTABILTIY & GOVERNANCE

9.1. Designation of DPO

The GDPR introduces a duty for entities to appoint a data protection officer (DPO), Tuya assigns such role and responsibility to a senior technical expert and privacy manager to monitor internal compliance work, inform and advise on data protection obligations, provide advice regarding technical and institutional measures implemented and act as a contact point for data subjects and the supervisory authority.

Annex I: Documentations for Further Reference:

No.	Name of the document	Description
1.	Privacy Policy	It includes Privacy Policy for different Tuya products and services, i.e. Apps, websites, etc.
2.	Security and Compliance White Paper	Tuya *Security and Compliance White Paper* is designed to introduce a comprehensive technological and infrastructural operation and ongoing maintenance of cloud service, security implementation and management, with the aim to provide Customers with in-depth understanding of Tuya security organization and security insights of Tuya Cloud. The document can be found HERE.
3.	GDPR Compliance Validation Summary	The summary letter issued by TrustArc validating Tuya privacy and compliance practices are conformed with the GDPR requirements. The letter can be found HERE.
4.	Standard Contractual Clauses	EU Standard Contractual Clauses for international data transfer (an agreement on the basis of approved per GDPR Art. 46). It can be found HERE.
5.	Tuya Data Processing Addendum(DPA)	The DPA is designed for Customers (a data controller) and Tuya (data processor), as well as the DPA for Tuya and its vendors (a subprocessor), by regulating any personal data processing conducted for contracted business purposes.
6.	Records of Processing Activity	Data Processing Activities according to Article 30 GDPR, the data inventory as well as its data processing records are documented and can be disclosed upon Customer or legal request.
7.	Tuya Data Retention Policy	Data retention policy concern what data should be stored or processed in different systems, where that should happen, and for exactly how long for the data that collected from end users. Once the retention time period for a particular data set expires, it shall be deleted or anonymized, depending on the requirements.

8.	Policy of Handling Individual Rights	This policy explains the rights the end users have by using Customer or Tuya services. This document provides information regarding how Tuya will fulfil our obligations under the GDPR. This document will also direct Customer to guidance which may be of assistance where appropriate.
9.	Incident and Data Breach Response Plan	A *incident and data breach response plan* is a document outlining how Tuya will respond in the event of a potential/actual data breach. It outlines what constitutes a cybersecurity and information security incident, or personal data breach, who is involved in the plan and steps to take in a breach and follow-up actions.
10.	Data Protection Impact Assessment (DPIA) Process Document	DPIA Template issued by Britain Information Commissionor's Office (ICO) and a sample of DPIA Assessment can be found HERE. A DPIA describes a process designed to identify risks arising out of the processing of personal data and to minimise these risks as far and as early as possible.
11.	Information Classification Guidelines and Matrix	The guideline is to establish a framework for classifying data based on its level of sensitivity, value and criticality to the Customer and its services as required by the GDPR or internal requirements. Classification of data will aid in determining baseline security controls for the protection of data.
12.	Business Continuity Planning (BCP)	A BCP is a system of prevention and recovery from potential threats to Tuya services. The plan ensures that personnel and assets are protected and are able to function quickly in the event of a disaster.
13.	Third Party Risk Management Policy (TPRM)	A TPRM policy uses the third-party risk management lifecycle to identify the risks that third parties introduce, Tuya creates a framework for what systems and types of data a third party can access based on particular service.