Brazil's Data Protection Law

Lei Geral de Proteção de Dados ("LGPD")

White Paper

June 2021

Tuya Inc.

The Table of the Content

Disclaimer

Brazil's new privacy law - Lei Geral de Proteção de Dados or the LGPD took effect September 18, 2020. Instead, the LGPD is entering into force now, although the penalties for infractions will only start being applied Aug. 1, 2021.

This document is a broad overview of the Lei Geral de Proteção de Dados ("LGPD"), the Brazilian General Data Protection Law, which took effective on September 18 2020. The documents also serves as a demonstration of how Tuya has been dedicated to comply with the LGPD. Before the enforcement of this law, Tuya spent great effort in the gap analysis and hard work on the remediation of such gaps. Evidence of conformance will be provided and welcome any enlightenment on the subject matter.

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 as a Controller

When Tuya collects personal data and determines the purpose and means of processing that personal data, when Tuya processes data from its direct customers, both individual customers and corporate customers, for account management, services access, service attributes, or contact information for the Tuya products and services for further support and administration, then Tuya acts as the data controller.

Tuya as an Operator

When customers and Tuya as a whole use Tuya services to process personal data in their customer content, Tuya plays as the operator (the data processor), our customers are the Controller. Customers and Tuya can user the controls available in Tuya services, including security configuration controls, to process and store personal data.

Using Tuya alone does not guarantee that customer fully complies with the LGPD, customers shall analyze their own business practices, technical and organizational measures to ensure compliance of the LGPD and ultimately hold the responsibility.

Applicability of the Law

According to the Law, there are three factors determining if the entities are applicable to be regulated by the law (Click any of the chckbox you may follow the LGPD):

☐ I – the processing operation is carried out in the national territory;

☐ II – the purpose of the processing activity is to offer or provide goods or services or the processing of data of individuals located in the national territory; or

☐ III – the personal data being processed were collected in the national territory.

This means that it is not just Brazilian citizens whose personal information is protected, but any individual whose data has been collected or processed while inside Brazil. Thus any entities that fall under the scope shall keep a close eye to the emergence and evolution of the LGPD.

Key Elements

Principles of Processing Activities

According to the Art.6 of the LGPD, the processing of personal data activities shall observe the following principles: a) purpose, b) adequacy, c) need, d) free access, e) data quality, f) transparency, g) security, h) prevention, i) non-discrimination, j) responsibility and accountability.

The principles shall be addressed not only in our daily business operation, as well as shall be kept transparent to all the data subject and let them know well the reason, the fundamental legal basis as well as the approaches of processing their personal data.

Conformance tracker	
Full implementation of Technical and Organizational Measures (TOMs)	*Tuya adopts and regularly reviewing the robust technical and organizational measures (which can be find in the Tuya Security White Paper) and Information Security Policies through the whole company.* *In order to ensure data adequacy, quality and security, as well as prevent data from inadvertent or advertent acts, Tuya has been dedicated to making every effort to ensure its compliance with domestic and international information security standards and legal requirements regarding personal data and privacy. Since the early stages of the company's operations, a comprehensive set of regulatory and compliance policies have been incorporated into our internal control framework, and we have diligently made, from time to time, additions and amendments to these policies to ensure that they are updated according to latest legislations and implemented subject to applicable requirements and standards.* *On a technical level, we have developed and designed our Tuya Cloud platform, products and services in accordance with applicable legal requirements and standards. Tuya Cloud secures infrastructure*

	management and operations as well as physical devices by selecting and working closely with the world's leading cloud hosting providers such as Amazon Web Services, Microsoft Azure. The data security mechanisms adopted by Tuya Cloud covers a comprehensive hierarchy of data and cloud services that are offered to our customers via the IoT platform. Tuya undertakes to leverage the expertise of its security team and globally recognized security service vendors in protective measures against external attacks, and technologies to provide full operational services for the Tuya Cloud platform, effectively protecting Tuya Cloud's secure operations and safeguarding customer privacy and data security.
PIA/DPIA or similar privacy impact assessment	Art. 38, The national authority may require the controller to draw up a report on the impact of the protection of personal data, including sensitive data, regarding its data processing operations, under the terms of the regulation, subject to commercial and industrial secrets. *In order to properly define the purpose and necessity of the data processing, Tuya will periodically conduct the PIA/DPIA, or similar privacy impact assessment so as to restrict the purpose limitation and data collection/usage minimization principle.* *Based on the nature of the business operation, a DPIA must be conducted when a business operation is likely to result in high risk, or the business operation entails large amount of personal data shall be deemed to have a DPIA in place.* *Corporate customers needs to conduct a DPIA because of collection of large quantity of personal data from the individual users, in the process of the assessment, Tuya has the obligation to assist the customer to fulfill the DPIA by providing information about the assessment mechanism or the concrete information about the personal data.*
Procedure of Handling Individual Privacy Rights	*Tuya has developed the Procedure of Handling Individual Privacy Rights, the internal process and products are refined for executing data subjects rights.* *LGPD emphasizes the protection and fulfillment of personal privacy rights. Tuya has formed the Procedures to help realize customer's privacy rights based on the provision of services. At the same time, Tuya also provides assistance to customers in responding to individual requests.*
Maintain a compliant Privacy Policy / Data Protection Policy	*Tuya maintains data privacy policy and keep the document updated, a record of the legal bases for processing of personal data have been recorded.* *Keeping the customers transparent and informed of Tuya governing*

	practices and obligations over processing their personal data is a pre-requsite when providing the products and services to customers. *The Privacy Policy can be found here for more: https://auth.tuya.com/privacy?from=http%3A%2F%2Fiot.tuya.com%2F.* *The Privacy Policy elaborates the type of personal data being collected and what service relies on these type of data, as well as the purposes of processing personal data.* *The prompt shall be displayed or a communication email shall be delivered to the users when a user registered in the App and, when the significant change has been made on the way or purposes of processing personal data, or on the new type of data collection, a separate consent shall be made by the user.*
Continuous Auditing efforts and other compliance endeavor	*Tuya compliance programs include:* ✓ *The Information Security Management System accredited by BSI, the leading information security standard organizer globally:* *ISO 27001, ISO27017, ISO27701, CSA-STAR certificate;* ✓ *The AICPA SOC2 TypeII Audit Report by Ernest&Young (E&Y);* ✓ *The GDPR (Generation Data Protection Regulation 2016/679) Validation Report issued by TrustArc, the leading privacy&compliance consulting firm in the industry;* ✓ *The CCPA (California Consumer Protection Act) issued by TrustArc;* ✓ *The Enterprise Privacy Certificate by TrustArc;* ✓ *The ETSI EN 303645 certificate issued by TUV SUD;*

Legal Bases

Article 7 et seq. of the LGPD contain the legal bases for data processing in Brazil, these include **consent from the data subject, legal obligation by the controller, public interest, research and social studies, protect health, as well as the legitimate interest and protection of credit.** Consent, as the fundamental legal bases lying the burden of proof for the data controller, according to Art.8, when the consent is provided in writing or by other means demonstrating the data subject's manifestation of will. Under such cases, an organization needs to properly document how and when consent was received, or how the company's interests are balanced against the rights of the individual.

In addition, the consent shall be for specific purpose, rather than generic authorizations. Therefore, the organizations shall sort out the different purpose of processing personal data, any purposes

rather than providing the defined products and services shall be providing the explicit way of gaining consent.

In Art.14, the processing of personal data of Children and Adolescents are also a fundamental issue for organizations to address. The principle of Consent and Transparency shall be strictly applied when conduct processing activities involved and shall validate the parent or legal guardian's consent if such processing is applicable to the organization.

For sensitive data elaborated in the Art.11, as well as for children's and adolescent's data, additional requirements apply. Two further explicit legal bases included in the LGPD are the use of personal data for the protection of credit, or for research purposes, ideally only until the data can be anonymized.

The processing of personal data through defected consent is forbidden. The law does not include any manifestation or examples of the type of being "defected consent".

Conformance tracker	
Consent mechanism	*Tuya develops different levels of consent mechanism over the utility of personal data: positive opt-in mechanism.* ✓ *The positive opt-in mechanism for data processing activities involving marketing solution and personalization;* ✓ *The consent are technically recorded once the customers have made a decision;* ✓ *Any decisions are easily for users to withdraw consent and the approaches are defined;* *The law grants the data subject the right to request a review of decisions taken solely on the basis of automated processing of personal data affecting his/her interests, (including decisions aimed at defining his/her personal, professional, consumer and credit profile or personality aspects), such information shall be made clear and adequate information regarding the criteria and procedures used for the automated decision, in compliance with commercial and industrial secrets.*
Deliver an independent privacy policy upon the children or adolescent if applicable	*It is required by the regulator that the organization shall disclose the data processing activities about children or adolescent, by distributing a notice page or separate paragraph.* *Even though Tuya does not identify adolescents or other special groups of people, we prepared such notice to individual users in the Privacy Statement.*

Information Classification and Handling Policy	*Tuya internally has a Information Classification and Handling Process to take care of different categories of data, including general data, data with limited access, and confidential data, i.e. personal data. Meanwhile Tuya would encrypt personal data in the database and desensitize when display on the database management platform, to lower the risk of data leakage.* *Tuya Cloud will logically isolate data to ensure the security of customer data. At the same time, Tuya Cloud provides different data storage services under various business scenarios. Personal data is encrypted and stored using AES256. Personal identity data will be desensitized and data categorized as highly sensitive will be secured with irreversible algorithm. At the same time, the key is uniformly secured through the key management system (KMS) and further managed and distributed through the KMS.* *For sensitive data, such as images or videos, Tuya will protect with generation of unique keys based on specific users and specific devices to encrypt the data.*
Data Processing Addendum or similar document serves the same purpose	Art. 39, The operator shall perform the treatment according to the instructions provided by the controller, who will verify compliance with the instructions and the rules on the matter. *Tuya has implemented the data processing Addendum upon the corporate relationship with the customer, under the term, Tuya and corporate customers are obliged to provide the state-in-art technical and organizational approaches, defined the roles and responsibilities between the two parties.*

The Data Processing Lifecycle

The data processing lifecycle may include form data generation, data collection, data processing (mixture of data processing techniques implemented), data removal.

The termination of processing pf personal data is occurred and shall be fulfilled under the following circumstances: 1) the purpose of processing personal data has been fulfilled and achieved, and data are no longer in use; 2) The end of the processing period; 3) Notice from the data subject to revoke the processing of personal data; 4) Determination of the national authority, when there is violation of the provisions of this Law.

Conformance Tracker

Inventory of Data Processing Activities	*Art.37, The controller and the operator shall keep a record of the personal data processing operations that they perform, especially when based on legitimate interest.* *Similar to other data protection regulations, the organization is required to document the processing of personal data from initial collection to termination, including details about a description of what is collected, the purpose of collection and processing, retention time and who the data is shared with.* *Tuya has prepared the Inventory of Data Processing Activities with regards to the data processing that we have both as a data controller and data processor. The data processing inventory may be disclosed with individual users or the corporate customer upon formal request.*
Data Security Lifecycle	*1) Data Collection* *Tuya adheres to the principles of data protection and personal privacy rights. The customer's consent for data collection constitutes the legal basis for data further processing. Data collection is performed by protecting the principle of transparency and the needs.* *2) Data Storage* *a) Data and File Storage* *Tuya Cloud will logically isolate data to ensure the security of customer data. At the same time, Tuya Cloud provides different data storage services under various business scenarios. Personal data is encrypted and stored using AES256. Personal identity data will be desensitized and data categorized as highly sensitive will be secured with irreversible algorithm. At the same time, the key is uniformly secured through the key management system (KMS) and further managed and distributed through the KMS.* *For sensitive data, such as images or videos, Tuya will protect with generation of unique keys based on specific users and specific devices to encrypt the data.* *b) Data Storage Location* *Tuya implemented 6 data centers, China Server Room, AWS West USA, Azure East USA, and AWS in Europe and India Server Room (with data centers physically isolated from each other) and a regional compliance data center in Russia, providing data services according to customer's location. More server rooms will be made available in the future.* ➢ *USA: Tuya has deployed two data centers in USA, the*

	west one in Oregon AWS, and the east one in MS Azure Virginia. By default, the data will be hosted in AWS while if the customer . ➢ *Europe: Tuya has deployed two data centers in EU, the AWS Frankfurt, Germany, and Azure in Netherlands.* *With more regional server centers are being constructed, more regional data center facilities are coming soon.* *c) Multi-copy Redundant Storage* *Under the distributed architecture, all servers are deployed simultaneously among three server rooms in different areas of the same city. Databases and other data storage services follow a multiple backup model (keeping a minimum of two real-time copies) that performs real-time backup. It allow high reliability and availability of data and services from the physical perspective.* *Tuya uses cloud databases for data storage, the default master-subordinate reproduction, the master and subordinate databases are distributed in different availability zones. All disks use local SSD hard disks and support automatic disk expansion. The full and incremental backups of data are all stored on cloud.* *For data backup and synchronization across computer rooms, strict data integrity checks will be performed to ensure the integrity of synchronized or backup data.* *3) Secured Data Processing* *a) Access Control Mechanism* *Tuya Cloud adopts access control mechanism relying on the Access Control Platform. Including the unified control of the application, and assigning the minimum and least necessary permissions according to the user roles and responsibility.* *Implement internal approval process for sensitive data operations.* *Separate the roles of security managers, data operators, and auditors.* *b) Data Filtering* *Tuya Cloud enforces strict verification of the type, length, format, etc. of the data of all entrances to ensure the integrity of the data and not be tampered.* *c) Data Auditing* *Complete data usage records, including auditing records of applications or user operations. For high-risk data processing, the*

	corresponding supervisor and compliance auditor needs to approve before it can be executed. *d) Data Desensitization* *After collecting personal data, Tuya will perform de-identification processing, and adopt technical and management measures to store the de-identified data separately from the data that can be used to restore the identification of the individual, and ensure that the subsequent processing of personal data does not re-identify the individual.* *4) Data Retention* *The retention period of personal information is the minimum time necessary to achieve the purpose for providing product and service. Tuya will delete or anonymize user data at the request of the customer, and return the data to the customer when the data retention policy triggers. Therefore Tuya has adopted the principle of minimum data retention:* ➢ *The retention of user's personal data is limited to the user's express consent so that the personal data can be used for service-related purposes, and shall not be used for any additional purposes without the user's consent.* ➢ *Data that needs to be retained in accordance with the law, or the company has the ability to prove that it is necessary for business purposes, can be retained within the time specified by a clear data retention schedule.* ➢ *Data retained for realizing the legitimate interests of customers or third parties can only be retained when the company has clear contractual agreements or instructions with customers or third parties, such as when providing services to customers or providing services for other purposes.* ➢ *According to the principle of minimum data retention, customers have the right to determine data retention strategies and inform Tuya in time for service purposes. When customers request to delete data or return data, Tuya will follow this clear instruction to execute.* *5) Elimination of Residual Data* *For any memory and/or disk that was once used for storage of customer data, the residual information will be automatically overwritten upon release and recovery. Any replaced or obsolete*

	storage device will be demagnetized and physically bent in unified manner by the cloud server infrastructure provider before being taken out of data center. *Once the memory and disk that have stored customer data are released and recovered, all their information will be automatically overwritten with zero values. At the same time, any replacement or obsolete storage devices will be degaussed and physically destroyed by the cloud server infrastructure provider.*

Data Subject Rights

The Art.9 is uniquely listed as one of the Data Subject Rights, the Right of Access.

In the response of Right of Access, the organization shall make available defined information that requested by the data subject.

Art. 18. of the Law specifies that "The personal data subject has the right to obtain the following from the controller, regarding the data subject's data being processed by the controller, at any time and by means of request", the individual rights are set out as the following: 1) confirmation of the existence of the processing; 2) access to the data; 3) correction of incomplete, inaccurate or out-of-date data; 4) anonymization, blocking or deletion of unnecessary or excessive data or data processed in noncompliance with the provisions of this Law; 5) data portability; 6) deletion of personal data processed with the consent of the data subject; 7) information about public and private entities with which the controller has shared data;8) information about the possibility of denying consent and the consequences of such denial; 9) revocation of consent as provided in §5 of Art. 8 of this Law.

The required response timeline applies to the controllers and operators that furthermore obliged both parties to provide transparent information on their data processing activities.

a) A simplified response (which is not defined in the law, but could for example include the statement that no data is held on the individual) needs to be provided ***immediately***.

b) For a more detailed response "that indicates the origin of the data, the nonexistence of record, the criteria used and the purpose of the processing, subject to commercial and industrial secrecy" the law ***foresees 15 days (yet not decided by the ANPD)***.

A large part of the LGPD is dedicated to the rights of individuals. The requirement is ever stringent in responding to the individual privacy request and lay a burden on the organization to execute and fully comply with the requirement.

Conformance Tracker

Procedure of Handling Individual Privacy Rights	*LGPD emphasizes the protection and fulfillment of personal privacy rights. Tuya has developed the Procedure of Handling Individual Privacy Rights, the internal process and products are refined for executing data subjects rights.* *At the same time, Tuya also provides assistance to customers in responding to individual requests.* *While it is worthy of attention that, previously Tuya shall respond the request within 30 calendar days or 15 business days, while LGPD requires the deadlines for dealing with individual requests for access may be less than this requirement. Therefore, Tuya will accordingly change the responding time by fully compliant with this law when the ANPD makes a clear conclusion.*

Personal Data Security Incidents

The LGPD includes a requirement to notify security incidents "that may create risk or relevant damage to the data subject" to the ANPD and the individuals themselves. The law does not include any further threshold for the breach notification.

Based upon the notification, the requirements of which are included in Article 48 of the law, the DPA may decide on further actions, including mitigation measures.

Conformance tracker	
Incident and Data Breach Response Plan	*Tuya has formulated the Incident and Data Breach Response Plan, to remediate and notify the data subject about the data breach.*

International Transfer of Personal Data

The LGPD allows the international data transfers only under the following cases:

I – to countries or international organizations that provide a level of protection of personal data that is adequate to the provisions of this Law;

II – when the controller offers and proves guarantees of compliance with the principles and the rights of the data subject and the regime of data protection provided in this Law, in the form of:

a) specific contractual clauses for a given transfer;

b) standard contractual clauses;

c) global corporate rules;

d) regularly issued stamps, certificates and codes of conduct;

VIII – when the data subject has given her/his specific consent and distinct for the transfer, with prior information about the international nature of the operation, with this being clearly distinct from other purposes.

As a main rule, transfers may take place to countries that have been declared as adequate by the Brazilian DPA. Thus, it depends on the authority to declare such countries in order to meet the cross-border transfer requirement. Adequacy shall be determined based on various criteria, including the applicable data protection regime and the nature of the data, but also alignment of security requirements with the LGPD, and "the existence of judicial and institutional guarantees for respecting the rights of personal data protection". Since the DPA has only just been established, it may take some time before we will see such adequacy decisions.

In the interim, or generally in absence of an adequacy decision for a country or international organisation, data can be transferred on the basis of sufficient guarantees the data will be protected (which includes the use of standard contractual clauses or ad hoc agreements, but also "global corporate rules", which would likely include BCRs and CPBRs).

The Brazilian DPA will in due course adopt Standard Contractual Clauses that can be used for international transfers.

Conformance tracker	
Follow the DPA to seek the countries or international organizations that provide a adequate level of protection of personal data	*At the current stage, data originates from Brazil will store in AWS USA by default; when it deems special demand from customers, for instance store data from Brazil in EU server, the reason is we deem the security and privacy safeguards are entirely under guaranteed when using the above data centers. When a customer raises exceptional requirement other than the above data centers, you may provide such justifications so that Tuya can follow.* *AWS, as a service provider, to a great extent helps ensure the fundamental security infrastructure of the data processing environment. For details how AWS help Tuya ensure the data security, you may see* https://d1.awsstatic.com/whitepapers/compliance/LGPD_Compliance_on_AWS.pdf *Once the DPA announces the list of countries or organizations, Tuya would adjust to follow and ensure its full compliance with the law.*

Follow the Standard Contractual Clauses (may be issued by ANPD)	*Since EU commission requires the organizations standard contractual clauses under GDPR, the Brazilian DPA has not issued the Brazilian version of SCC yet, and it may await the mature of the data protection framework, it is required to put ahead the international transfer terms in the data processing activities when contracted with individuals, as well as between corporate customers.*
Transparency about international data transfer	*As a data controller, whether it's Tuya or the corporate customer, you may inform the individual users about the international data transfer in a explicit and transparent way, for instance, in the Privacy Policy.*

Accountability

Art. 40, The national authority may provide for interoperability standards for portability, free access to data and security, as well as for record keeping time, with particular regard to necessity and transparency.

Additional Governing Rules from ANPD

The national authority may lay down ***minimum technical standards (frequently checking the*** to make the provisions of the main section of this article applicable , taking into consideration the nature of the information processed, the specific characteristics of the processing and the current state of the technology, especially in the case of sensitive personal data, as well as the principles provided for in the caput of art. 6 of this Law.

Rule of good practice and governance

Controllers and operators, within the scope of their competences, for the processing of personal data, individually or through associations, may formulate rules of good practice and governance that establish the conditions of organization, the operating regime, the procedures, including holder complaints and petitions, safety standards, technical standards, specific obligations for the various parties involved in processing, educational actions, internal supervisory and risk mitigation mechanisms and other aspects related to data processing personal.

The LGPD stipulates in Article 6(X) that accountability is one of the key principles to which data processing operations by controllers and processors shall be subject. According to the provision, this requires the controller or the processor to be able to demonstrate "the adoption of measures which are efficient and capable of proving the compliance with the rules of personal data protection, including the efficacy of such measures". A similar requirement can be found in Chapter IV, Section II, for public authorities. Both requirements are rather similar to the accountability requirement that can be found in the EU GDPR, and also comes with an obligation in Article 37 to maintain a processing activities register. In addition, data controllers can be asked

to prepare an impact report for data processing operations, which should include descriptions of security measures and risk mitigation. When such assessments will be mandatory will be defined by the DPA, which will also determine when a Data Protection Officer will need to be appointed. A notable section of the LGPD related to accountability can be found in Article 50(1)I, which suggests the elements that organizations can use when building a privacy governance program. These vary from demonstrating "the controller's commitment to adopt internal processes and policies that ensure broad compliance with rules and good practices regarding the protection of personal data" to "establishing adequate policies and safeguards based on a process of systematic evaluation of the impacts on and risks to privacy". When doing so, organizations will need to take into account relevant risk factors, such as the structure, scale and volume of their operations, as well as the sensitivity of the data. Furthermore, the privacy governance program will need to be integrated in the general governance structure of the organization and be updated on a regular basis.

Conformance tracker	
The security and compliance team	*Tuya has an in-house security technology team, which is composed of the former members from leading internet companies, conventional security manufacturers. For the formulation of compliance team, we have member of privacy officer, who experienced in the data privacy and was served a US financial service company. Meanwhile, Tuya invited external professional privacy and security consultancies on the subject matter to ensure the security & compliance ecology.* *The team as a whole, working with Tuya legal team, ensures that the architecture of security and compliance is under controlled, and reliable at each granular perspective.*
Security Risk Assessment and Management	*Tuya security team taking charge of vulnerability management and discovery, which is able to discover, track, trace and fix security vulnerabilities.* *Tuya's security team conducts security penetration tests before any business code is online; meanwhile, and periodically conducts black-box testing for online business.* *Each year Tuya also cooperates with third-party security organizations to complete penetration testing on cloud services, mobile clients, hardware products, and even throughout the company IT infrastructure as a whole.* *Tuya supports external white hats to submit vulnerabilities through Tuya SRC (https://src.tuya.com/) or external security email contacts, and provides the submitter with a vulnerability bonus of up to $100,000 for a single high-quality and high-risk vulnerability. Tuya will verify and evaluate the vulnerability internally and if it is indeed a vulnerability, it will track the vulnerability repair through a work order until it is*

	completed, Tuya will report the entire process to the white hat. *The vulnerability scores are comprehensively rated in accordance with the technical requirements of attack, the scope of impact, the complexity in discovering and using the vulnerability, the importance degree of corresponding business, and the possible damage of the vulnerability as specified in the Tuya's Vulnerability Risk Rating and the CVSS3.1 for internal vulnerability risk rating.* *If the vulnerability involves the App and hardware, the fix timeline can be referenced with Tuya SLA.*
Access Control	*Tuya implements unified management of system permissions, machine permissions, data permissions and other permissions of the IT system, and realizes a zero-trust permission management model. Based on the types of user identities, application identities, and application functions, it achieves minimal permission control.* *1) Authentication, Authorization, Accounting* *The system permissions mainly include internal system platform permissions, application permissions, and machine permissions. The authorization of system permissions follows the "principle of minimum privilege", that is, to assign each authority role and only assign the "essential" authority needed to complete the task or operation. At the same time, the system strictly records all audit records for changes in permissions.* *Regarding the identity authentication of the internal system, Tuya has implemented single sign-on (SSO) for all internal applications. At the same time, SSO realizes the ability of OTP. In addition to meeting all password management requirements, it also increases the dynamics of each login. Code verification capability.* *Tuya has a unified authority management system (ACL) for the access verification of the internal system, which realizes the authorization of applications, application functions and data. There is a complete approval process management on the platform.* *2) Access Control on Machines* *Tuya employees have a unified management platform for machine permission application and approval. The approval of the corresponding supervisor, operation and maintenance, security and application person in charge is required to complete the authorization. After the employees are authorized, they can log in to the Jumpserver to control the limited access of the machine. At the same time, the authorization approval process, machine login session, command, file transfer, etc. have a complete audit*

	process. *3) Access Control on Applications* *Tuya implements unified management and control of permissions for each application and calls between applications. The service access of Tuya's internal applications requires the use of a unified client component, through which the mutual identification of user identities and the control of permissions are realized. Application authentication is realized through a unified authentication service.* *4) Access Control on Database* *Tuya's database authority management mainly includes: application accounts, database platform accounts, etc. The application account refers to the account provided for the application to access the database, and the identity authentication is realized by identifying the machine where the application is located.* *The accounts used by the database platform are specially created by the DBA, including read-write permission used to execute work orders and read-only accounts used by query modules. The database platform accounts are rotated every 3 months.*
Security Management of Service Provider	*1) the Risk Assessment of Service Provider* *Tuya has formulated a screening mechanism and regular evaluation mechanism for platform software vendors. In addition to the security indicators of hardware products and the security standards of software services, Tuya needs to have a deeper understanding of the practices of various service providers in information security assessment and privacy compliance. The information security assessment involves security penetration testing and supplier security capability assessment. For details, please refer to Section 5.4.* *2) the Monitoring of Service Provider* *Real-time monitoring over the service quality, paying attention to the third parties security management, etc., so that Tuya can respond quickly when abnormalities occur.*
Security Awareness and Discipline	*To enhance the network security awareness of all the employees, avoid network security violation risk, and ensure normal business operation, Tuya has released Information Security Manual for Employees of Tuya Smart, based on which employee education of network security awareness is held regularly, and all the employees are required to study network security knowledge continuously to understand the policies and systems in the manual, keep in mind what activities are acceptable or unacceptable,*

	be aware of taking responsibility of their activities even without subjective intention, and make the commitment to behaving as required. *Tuya "Employee Information Security Handbook" supports employees' security awareness and code of conduct, a quarter assessments and education will be conduct which aims to regulate employees' disciplines over handling information security matter. Public commendation or warning will be given to employees who exceeding the expectation on information security protection or who violate security policies and procedures.*

Appointment of the Data Protection Officer (DPO)

Art.41, The controller shall appoint the a DPO or a personnel with the similar role for the processing of personal data.

The law requires the identity and contact information of the officer shall be publicly disclosed, in a clear and objective manner, preferably on the ***controller's website***.

The responsibilities of the DPO is defined under the LGPD:

I – accepting complaints and communications from data subjects, providing explanations and adopting measures;

II – receiving communications from the national authority and adopting measures;

III – orienting entity's employees and contractors regarding practices to be taken in relation to personal data protection; and

IV – carrying out other duties as determined by the controller or set forth in complementary rules

Conformance tracker	
Appointment of a DPO and contact details for the DPO or Privacy Office	*Tuya Privacy Policy has declared the contact information of Tuya Privacy Office, which is in charge of by DPO and privacy office, who is conducting routine monitoring of privacy work and communication with authorities about the endeavors Tuya has created.* *The corporate customer shall appoint such role for responsible for internal privacy and compliance matters as well and make the information transparent for DPA and individual user.*

Oversight

The Brazilian Data Protection Authority, the National Authority for Data Protection or "ANPD", was established by a decree based on the LGPD. The ANPD will fall directly under the presidency of the Republic, and has as main objective "to protect the fundamental rights of freedom and privacy and the free development of the personality of the natural person". Furthermore, the ANPD will have technical and decision-making authority, which serves to provide the implementing guidelines under the LGPD, for example to further guide the rules related to international data transfers or to impact and risk assessments.

Enforcement

The supervisory authority: National Data Protection Authority will be created and governing with more power.

Controllers and operators that do not meet the requirements of the LGPD may be confronted with serious fines, as of August 2021. Apart from possible warnings, the blocking of processing activities and the publication of the contravention, the law foresees fines of up to 2% of the company's revenue in Brazil in the previous year (either at company, group or conglomerate level), with a maximum of 50 million reais (~ USD 9 million). In more serious situations, that maximum would apply to a daily fine, which could likely be imposed until the contravention is ended. As an additional sanction, the DPA is allowed to publish the committed infraction of the law.

Any infringement of this law may result in the suspension of the processing of personal data for a maximum period of six (6) months, which is extendable. In a worse condition of violation, partial or total data processing activities may be prohibited.

Conformance tracker	
Keep Track with the Enforcement	*In order to collaboratively respond to the DPA and conform with the law, Tuya pays high attention to fulfill with the obligations lying in Tuya and its corporate customers.* *Since the DPA guidelines on key conformance trackers have yet to be created, these cannot yet be completed. However, Tuya can make a first determination of the likely high risk processing operations, and document what risks they see and how these are mitigated. Once the DPA guidelines are available, it will take less time to complete the full risk and impact assessments.*

Key Definitions in the Law

In this whitepaper, some of particular definitions shall be given prior attention as clearly defined in the LGPD and will appear in the document, the terms not listed below but adopted in the document shall have the same meaning as in LGPD.

Personal Data: any information relating to an identified or identifiable natural person

Unlike the GDPR, there are no examples on the definition outlined by the law, leaving this open for future interpretation by the Brazilian National Data Protection Authority, the public agency responsible for supervising, implementing and monitoring the compliance with the LGPD

Sensitive Personal Data: personal data on racial or ethnic origin, religious conviction, political opinion, union affiliation or religious, philosophical or political organization, health or sexual life data, genetic or biometric data, when linked to a natural person

Anonymized Data: Fully outlined under the LGPD, data are considered to be anonymous, when "reasonable and available technical means" at the time of the processing are used to remove the possibility of direct or indirect association with a natural person

Meanwhile, the data that are confirmed anonymized which could not be reversed by all means it takes, are not considered as Personal Data

Data Subject: Under the LGPD, a data subject is a "natural person to whom the processed personal data refer."

Controller: a controller is a "natural person or legal entity, of public or private law, that has the competence to make decisions regarding the processing of personal data."

Operator: a "natural person or legal entity, of public or private law, that processes personal data in the name of the controller."

Person in charge: person appointed by the controller and operator to act as a communication channel between the controller, the data subjects and the National Data Protection Authority (ANPD)

Blockade: temporary suspension of any processing operation, through the blockage of personal data or the database

Impact Report on the Protection of Personal Data: controller's documentation containing a description of personal data processing activities that may pose risks to civil liberties and fundamental rights, as well as risk mitigation measures, safeguards and mechanisms;

Similarly, it is a form of privacy impact assessment shall be prepared and maintained by the

controller

Consent: Similar to the GDPR, consent is a "free, informed and unambiguous manifestation whereby the data subject agrees to her/his processing of personal data for a given purpose." Consent shall in principle be in writing, or in another way that demonstrates the data subject's manifestation, shall be distinguishable from other contractual clauses and needs to be properly documented. It may be revoked at any time.

End of document