Tange Intelligent Privacy Protection Whitepaper

Shenzhen Tange Intelligent Technology Co., Ltd.

2026/6/8

Content

Preface

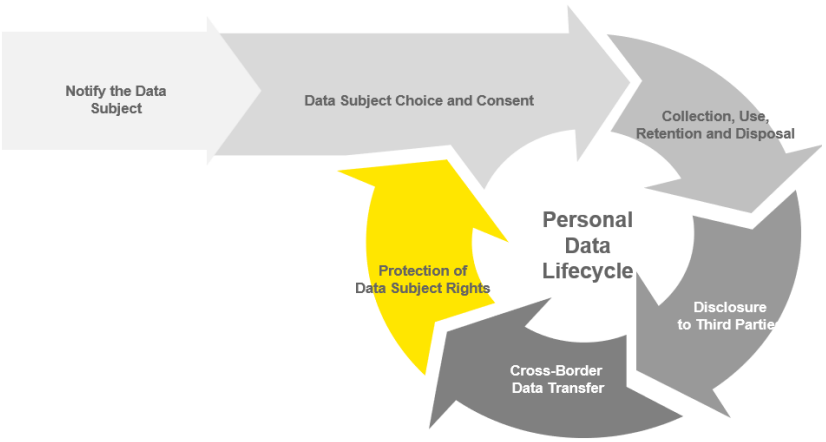
Shenzhen Tange Intelligent Technology Co., Ltd. (hereinafter referred to as "Tange") is an IoT audio/video PaaS and data service provider, founded on October 23, 2018. It delivers services to IoT device manufacturers, brand customers, solution providers, and external developers through the Tange Intelligent IoT Audio and Video Cloud Platform. The service provides embedded real-time audio/video communication, device access, cloud storage, 4G connectivity, AI event search, AI event summary, object recognition, Open API and SDK capabilities.

Tange places a high priority on privacy protection, strictly adhering to the EU's *General Data Protection Regulation* (GDPR) and the *California Consumer Privacy Act* (CCPA), while continuously monitoring applicable privacy laws and regulations across various countries and regions globally. To support this commitment, a comprehensive privacy governance framework has been established, commensurate with our business scale and data risk profile.

This white paper, grounded in the regulatory frameworks of the GDPR and CCPA, systematically outlines Tange's privacy practices across the following 11 core domains:

- Internal Privacy Policy and Organization
- Risk Management and Security of Processing
- Privacy Audit and Monitoring
- Privacy by Design
- Lawfulness of Processing
- Data Subject Rights
- Third-Party Management
- Cross-Border Data Transfers
- Appropriate Retention and Disposal
- Breach Management
- Training and Awareness

Anchored in the concept of full-stack personal data lifecycle management, this document aims to demonstrate Tange's comprehensive privacy protection management system to all stakeholders.



Full-Stack Management of the Personal Data Lifecycle

Tange's Fundamental Principles for Processing Personal Information

Tange has established fundamental principles for personal data processing in accordance with applicable laws and regulations. Through appropriate management and technical measures, Tange ensures compliance with the following core principles when processing personal data:

- **Purpose Specification**: Personal data shall be processed for specific, explicit, and legitimate purposes.
- **Openness and Transparency**: The scope, purposes, rules, and other details regarding personal data processing shall be disclosed clearly, understandably, and reasonably, ensuring accountability through appropriate oversight.
- **Choice and Consent**: Data subjects shall be explicitly informed of the purposes, methods, scopes, and rules of processing, and their explicit authorization and consent shall be obtained prior to any processing activities.
- **Data Minimization**: Only the minimum amount and type of personal data necessary to achieve the specified purpose shall be processed.
- **Storage Limitation**: Personal data shall be retained only for the shortest period necessary to achieve the processing purposes.
- **Security Assurance**: Adequate security capabilities commensurate with the risk levels shall be maintained, supported by robust management measures and technical safeguards to ensure the confidentiality, integrity, and availability of personal data.
- **Data Subject Participation**: Convenient channels shall be provided to facilitate the exercise of data subjects' rights, including the right to access, rectify, or delete personal data, as well as to withdraw consent, close accounts, and file complaints or reports.

Privacy Protection Management System

Internal Privacy Policy and Organization

Tange has established a comprehensive privacy and data compliance policy, which is centrally maintained on Feishu and made available to all employees. The policy covers key areas including data subject rights, data processing principles, the collection, storage, use, sharing, disclosure, and transfer of personal information, cross-border data management, privacy impact assessments, emergency response protocols, and the scope of application for privacy protection.

Furthermore, Tange's Information Security and Privacy Management Team conducts an annual compliance review against applicable laws and regulations to ensure the continued effectiveness and relevance of this policy.

To ensure the effective operation of the aforementioned system, Tange has established a dedicated Information Security and Privacy Protection Management Committee and an Information Security and Privacy Management Team. These bodies are responsible for the comprehensive design, implementation, enforcement, and continuous optimization of the Company's information security and privacy framework.

The Committee is composed of the Company's General Manager, senior executives as stipulated in the Articles of Association, and the System Management Representative. The Management Team consists of cross-functional members.

The daily governance and protection of personal data are managed by the Information Security and Privacy Management Team. Its core responsibilities include:

- **Overall Coordination:** Comprehensively coordinate the Company's personal information protection efforts, formulate and update personal information management policies;
- **Data Inventory and Access Control:** Establish, maintain, and update an inventory of all personal information held by the organization (including type, volume, source, and recipients), and define authorization strategies for access;
- **Risk Assessment:** Conduct Personal Information Security Impact Assessments, propose protective measures, and oversee the rectification of security risks;
- **Training and Awareness:** Organize and conduct training sessions on personal information security;
- **Complaint Handling:** Publish channels for complaints and reports, and promptly address relevant feedback;
- **External Communication:** Maintain communication with relevant regulatory and supervisory authorities, and timely report or notify them regarding personal information protection matters and incident response.

Furthermore, to strictly adhere to GDPR requirements, Tange has appointed an independent Data Protection Officer (DPO), who reports directly to senior management. The DPO's core responsibilities include:

- **Compliance Oversight:** Monitor the Company's data processing activities, regularly organize Privacy Impact Assessments (PIA) and Data Protection Impact Assessments (DPIA), and provide professional recommendations;
- **Regulatory Liaison:** Serve as the primary point of contact between the Company and data protection authorities, assisting in responding to regulatory investigations or audits;
- **Data Subject Rights Response:** Establish and optimize processes for responding to data subject rights requests to safeguard data subjects' rights;
- **Training Coordination:** Plan and organize specialized data protection training sessions for employees;
- **Record Keeping and Reporting:** Maintain detailed records of the organization's data processing activities and report regularly to top management.

Risk Management and Security of Processing

To ensure that the Tange Cloud Platform continues to effectively support business operations while fully complying with applicable laws and regulations, the Company has implemented a comprehensive risk management framework designed to proactively identify, assess, manage, and monitor potential information security and privacy risks.

The Company has established internal management systems that clearly define employees' responsibilities regarding risk identification, assessment, and mitigation to ensure effective risk control.

On the execution level, the Human Resources team collaborates annually with all business departments to comprehensively review core information assets within existing business operations. From multiple dimensions including business operations, fraud prevention, internal controls, information system security, and privacy compliance, the team conducts in-depth analysis to identify potential risks that could negatively impact these core assets.

All identified risks are assigned to dedicated responsible teams for tracking and remediation. Ultimately, the entire assessment process and its results are consolidated into a comprehensive information security and privacy risk assessment report.

Building on the implementation of these policies, and to further strengthen the security of data processing, Tange implements technical and organizational measures commensurate with the level of data risk. These measures are designed to comprehensively prevent the accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or access to personal data during its transmission, storage, and processing.

At the data transmission and storage levels, Tange employs HTTPS and DTLS protocols to ensure secure transmission. Sensitive personal data and core business data are stored using encryption and logical isolation. For high-sensitivity fields such as mobile phone numbers, de-identification techniques or industry-standard protection algorithms are applied during storage to prevent unauthorized direct access.

In terms of identity and access control, the Company enforces strict governance based on the principle of least privilege, complemented by signature-based security validation and token management mechanisms to ensure that only authorized personnel can access relevant data resources. Furthermore, Tange regularly conducts system vulnerability scanning, penetration testing, and security baseline assessments. Any identified risks are addressed through immediate remediation and subsequent re-verification, thereby ensuring a sustained secure posture.

Privacy Audit and Monitoring

To ensure the continuous improvement of privacy protection, Tange has established a comprehensive audit mechanism. At the policy level, the Company has formulated a dedicated audit management system that clearly defines the inspection principles, audit frequency, and management procedures that must be followed when conducting information security and privacy protection audits.

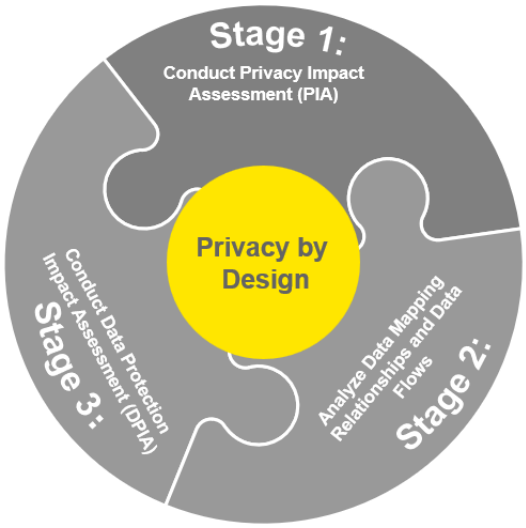
Building on this foundation, the Company formulates a specific privacy protection audit plan annually. This plan clearly defines the audit scope, which covers internal controls, information security, and privacy protection, along with the execution timeline and participating teams to

ensure that audit activities are carried out in an orderly manner. Upon completion of the audits, the Company produces formal audit reports.

For any issues identified during the audits, the Human Resources team collaborates with relevant business departments to conduct root cause analysis, confirm corrective action plans, and implement follow-up measures. These steps ensure the effectiveness and continuity of the internal control system.

Privacy by Design

Tange has established a comprehensive risk assessment process for privacy data protection. Adhering to the Privacy by Design principle, the Company integrates privacy protection throughout the entire lifecycle of the Tange Cloud Platform.



Continuous supervision and management are performed by Tange's Information Security and Privacy Management Team

When the platform plans to introduce new technologies, launch new features, or adjust existing technical architectures and functionalities, the Company conducts a PIA during the requirements analysis and functional design phases prior to the formal commencement of development. The scope of this assessment covers the following key aspects:

- **Types of Personal Data Involved:** Including sensitive information such as criminal conviction records, genetic data, political opinions, or religious beliefs;
- **Purpose of Data Processing:** Clearly defining the specific objectives for collecting and processing personal data;
- **Data Volume:** Assessing the scale of personal data to determine whether it constitutes large-scale processing;
- **Cross-Border Transfers:** Situations involving the cross-border flow of personal data;
- **Automated Decision-Making:** Scenarios involving automated decision-making and profiling;
- **Third-Party Integrations:** Usage of cookies, social media integrations, or third-party open-source platforms;

- **Application of New Technologies:** Incorporating new technologies or solutions into information processing activities; and
- **Protection of Children's Information:** Collection of information related to children's social services.

Based on the results of the PIA, the product team must first complete the compilation of data inventories and data flow diagrams to clarify the purposes of data processing and existing control measures. If the assessment confirms that the proposed new technologies, features, or adjustment plans may pose a high risk to the rights and freedoms of natural persons, such as when involving the handling of sensitive personal information, the Company will further initiate a DPIA.

Through the DPIA process, the Company identifies the specific technical functions required for each version to ensure personal data security and compliance. Prior to launch, these functions undergo strict review to verify their completion status and effectiveness. Additionally, the Company retains comprehensive records of the entire evaluation process for every instance, establishing a traceable management loop.

The DPIA process encompasses five core dimensions:

- **Overview of Information:** Clarifying the data collection and processing activities involved in the version's functions, including the purposes of processing, types of operations, categories of data and data subjects involved, as well as details regarding information systems and third-party processors;
- **Necessity Assessment:** Rigorously reviewing whether data processing adheres to the principle of data minimization to ensure that collection activities are reasonable and necessary;
- **Risk Identification and Assessment:** Comprehensively identifying potential risk points and conducting both qualitative and quantitative assessments;
- **Development of Mitigation Measures:** Formulating targeted mitigation measures for identified risks and implementing corresponding security safeguards;
- **Documentation and Archiving:** Standardizing and archiving the assessment process and conclusions to provide a reliable basis for pre-launch audits, accountability, and subsequent optimization.

In addition to the specialized assessments conducted for routine iteration projects, Tange has also established a normalized periodic evaluation mechanism. Annually, the Company conducts comprehensive DPIA on personal information processing activities within existing business operations. This process involves a thorough review of data processing activities, field types, and workflows across all platforms to effectively implement the "minimum necessary" collection principle.

Furthermore, Tange regularly evaluates Records of Data Processing Activities (RoPA) and reports the evaluation results to relevant stakeholders. For any identified procedural deficiencies, the Company promptly formulates improvement plans and completes process

optimizations to ensure continuous compliance.

Lawfulness of Processing
Tange strictly defines the applicable legal basis according to different business scenarios and purposes of data processing. When designing specific or optional features, such as requesting access to the camera, microphone, and location services, Tange always prioritizes the autonomous choice of data subjects and implements relevant data processing activities only after obtaining explicit consent.

For the delivery of Tange Cloud Platform's core services, Tange processes personal data as necessary for the performance of a contract. Additionally, to fulfill statutory obligations, Tange processes necessary data in accordance with applicable laws and regulations in scenarios such as mandatory regulatory compliance.

Furthermore, provided that a thorough assessment is conducted to ensure that the rights and freedoms of data subjects are not infringed upon, Tange may process personal data based on its own legitimate interests or those of third parties. Examples include conducting internal data analysis to optimize service quality.

Data Subject Rights
Tange places high importance on data subjects' rights to manage their personal information and is committed to assisting them in effectively managing such data by providing convenient, transparent, and compliant mechanisms for exercising these rights. To this end, Tange clearly discloses the relevant response channels for exercising these rights within its Privacy Policy.

Tange fully supports data subjects in exercising their rights, including the right to be informed, the right to consent, the right of access, the right to rectification, the right to erasure, the right to data portability, the right to object, and the right to restriction. Tange has established a standardized privacy request response process. To address different data processing scenarios, Tange implements differentiated collaborative mechanisms:

- **In Entrusted Processing Scenarios:** Tange will promptly escalate issues to the entrusted party, who is responsible for following up and resolving them.
- **In Joint Processing Scenarios:** Tange has established a comprehensive end-to-end response mechanism covering request receipt, identity verification, reasonableness assessment, data retrieval, processing execution, and notification feedback. In principle, this process will be completed within one month. If sharing data with third parties is required to fulfill the request, Tange will immediately notify the third party of the relevant requirements upon receiving the request, urge them to complete the handling in accordance with the data subject's exercise of rights, and provide the processing results to the data subject within the agreed timeframe.

Furthermore, the Company has clearly defined in its policies the scenarios and content specifications under which data subjects may obtain copies of their information. If a copy is required, authorized personnel will export or provide the relevant information in accordance

with established procedures and strictly adhere to accuracy verification procedures.

For requests from data subjects to withdraw consent or restrict data processing, the Company follows the disposal procedures established for joint processing scenarios. Upon receiving such a request, the Company manually flags the affected data to ensure that further analysis and processing are restricted, and completes the response within the specified timeframe.

Finally, in accordance with the relevant provisions of the GDPR and CCPA, Tange reserves the right to lawfully restrict or reject requests that are manifestly unfounded, excessive, or in conflict with legal obligations. The Company will provide data subjects with specific reasons for such decisions within the prescribed response timeframe.

To ensure full traceability throughout the process, Tange will record and archive all handling activities related to data subjects' rights requests. These records will be retained for a period of 24 months to facilitate subsequent verification by data subjects or regulatory authorities.

Third-Party Management

Tange establishes partnerships with third-party vendors only if they possess robust data security protection capabilities and can implement appropriate technical and organizational measures.

During the onboarding phase, Tange establishes a standardized partner access process that includes conducting privacy compliance assessments to ensure vendors meet all qualification requirements. For suppliers involving overseas data subjects or new partnerships, Tange mandates the signing of Data Processing Agreements (DPAs) to clearly define the legal liabilities and protection obligations of both parties regarding data transmission, storage, and processing.

During the partnership, Tange establishes and maintains an up-to-date vendor list, designating specific personnel to conduct regular monitoring and periodic spot checks. Additionally, Tange conducts annual information security reviews of its vendors to ensure ongoing compliance.

Cross-Border Data Transfers

Tange is committed to providing global services, with operations spanning multiple overseas regions. Subject to obtaining data subject consent or complying with applicable laws and regulations, certain information may be transferred to jurisdictions outside the data subject's country or region of residence, or accessed from overseas locations.

To effectively safeguard the security and compliance of cross-border data transfers, Tange has constructed a comprehensive protection system across three dimensions: contractual agreements, technical safeguards, and process controls.

- **Contractual Level:** Tange signs Standard Contractual Clauses (SCCs) or DPAs with data recipients to clearly define the division of responsibilities and mechanisms for liability in case of breach.
- **Technical Level:** Tange employs HTTPS secure transmission protocols and implements

encryption at the transport layer.

- **Process Level:** Tange has established cross-border data transfer review standards, mandating that a security assessment be completed prior to any data leaving the country. The scope of this assessment covers the purpose of transfer, specific data fields, data volume, the legal basis for processing, the destination jurisdiction, and the security qualifications of the recipient.

Appropriate Retention and Disposal

Tange adheres to the principle of data minimization, retaining personal data only for the shortest period necessary to fulfill the purposes of processing. To this end, Tange implements a classified and tiered control strategy for data retention:

- **For Unstructured Business Data:** Tange configures lifecycle management policies within its object storage services, strictly adhering to predefined retention rules to automatically delete data upon expiration;
- **For Account Credentials:** Upon termination of a user's APP account, the system automatically triggers the deletion process for account credentials;
- **In Response to Data Subject Rights Requests:** When a data subject exercises their right to erasure, designated personnel manually execute the deletion operation while simultaneously retaining comprehensive deletion logs for audit purposes.

If otherwise required by law, or to comply with the enforcement actions of government agencies, court judgments, or rulings, the data retention period may be extended in accordance with applicable laws.

When personal data is no longer necessary for processing, Tange will implement appropriate technical and organizational measures to permanently delete or anonymize the data, thereby effectively mitigating the risks of unauthorized access or leakage.

Breach Management

Tange has established a comprehensive data breach response and handling mechanism to effectively address personal data breach incidents. Upon the occurrence of a data breach, Tange will immediately activate its emergency response procedures to conduct a risk assessment and classification of the breach.

- If the assessment determines that the breach poses a high risk to the rights and freedoms of natural persons, Tange will report the incident to the relevant regulatory authorities in accordance with statutory procedures within 72 hours of becoming aware of the breach;
- If the breach poses a high risk to data subjects, Tange will notify the affected data subjects without undue delay.

To strengthen the closed-loop management and continuous improvement capabilities of incident response, Tange maintains detailed records and archives for all personal data breach incidents. These records cover the factual sequence of events, impact assessments, and remedial measures taken. For representative incidents, IT personnel will lead cross-departmental post-incident review meetings to conduct in-depth root cause analysis and formulate improvement measures.

Furthermore, Tange places great emphasis on proactive prevention by identifying potential data breach risks based on business scenarios and classifying them according to severity levels to develop corresponding emergency drill plans. Tange conducts at least one data breach emergency drill annually and produces a specialized report and post-drill review following each exercise to ensure continuous optimization.

Furthermore, Tange clearly defines the responsibilities and obligations of partners regarding data breach incidents within the DPAs signed with them, ensuring consistency across the security defense lines throughout the supply chain.

Training and Awareness

The Company analyzes the personal information protection compliance requirements that need to be addressed, taking into account business development trends, operational scale, and the countries and regions involved. Based on this analysis, it continuously refines its general compliance training system and conducts specialized training sessions as needed on an irregular basis.

Additionally, the company has established a post-training assessment mechanism to evaluate employees' knowledge retention. This initiative aims to comprehensively enhance information protection awareness across the entire organization and effectively mitigate compliance risks.

Conclusion

In an era of rapidly accelerating IoT development, data has become the core driver of innovation, while privacy protection serves as the cornerstone of technological trust. Tange consistently places user privacy at the heart of its business strategy. Tange not only strictly complies with major global privacy regulations such as the GDPR and CCPA, but also has established a comprehensive privacy governance framework spanning the entire data lifecycle, including collection, processing, storage, secure disposal, and response, through the deep integration of robust policies, dedicated organizational structures, advanced technical safeguards, and a strong privacy-aware culture.

Tange recognizes that compliance is not a destination, but a continuous journey of evolution. Looking ahead, Tange remains committed to sustained investment in privacy-enhancing technologies, proactively aligning with emerging regulatory landscapes and industry best practices. Together with our customers and partners, Tange will co-create a trusted, resilient, and sustainable future for the intelligent IoT ecosystem.

Appendix 1: Glossary of Terms

- **Anonymize:** The irreversible processing of personal data (e.g., through k-anonymity, differential privacy, or strong cryptographic hashing) such that the data subject can no longer be identified, and the original data cannot be reconstructed.
- **Data Subject:** A natural person who is identified or identifiable by reference to personal data.
- **Data Protection Officer (DPO):** An independent compliance expert established within the organization, responsible for overseeing the implementation of data protection strategies, monitoring compliance, and serving as the liaison between the enterprise, regulatory authorities, and data subjects.
- **Data Protection Impact Assessment (DPIA):** A systematic, proactive assessment conducted prior to high-risk data processing activities (e.g., large-scale monitoring, automated decision-making, or cross-border data transfers) to evaluate risks to data subjects' rights and freedoms and implement necessary safeguards.
- **De-identification techniques:** The processing of personal data through technical measures (e.g., masking, hashing, or tokenization) such that the data can no longer be attributed to a specific natural person without the use of additional information, which is maintained separately and subject to appropriate safeguards.
- **Data Processing Agreement (DPA):** A legally binding contract executed between Tange and third-party partners that explicitly defines the purpose, methods, scope, rights, and obligations of data processing, as well as protocols for security incident management and breach notification. Execution of a DPA is a statutory prerequisite for entrusted or joint processing scenarios.
- **Privacy Impact Assessment (PIA):** A systematic evaluation conducted prior to the implementation of a system or project involving the collection, use, or disclosure of personally identifiable information (PII), designed to identify potential privacy risks and establish appropriate mitigation measures.
- **Record of Processing Activities (RoPA):** A comprehensive register maintained by Tange in accordance with applicable laws, documenting key elements of data processing activities including purposes, data categories, retention periods, and security measures. This record serves as a foundational document for internal audits and regulatory inspections.