TTS-US PRIVACY POLICY

I. Purpose

Toyota Tsusho Systems – US ("TTS-US") has adopted this Privacy Policy ("Policy").

This Policy:

- sets forth the principles that apply to the Processing of Personal Information by TTS-US, and describes how TTS-US adheres to these principles; and
- provides an overview of TTS-US's privacy governance structure, and the roles and responsibilities of key individuals and groups in carrying out TTS-US's privacy compliance obligations and tasks.
- summarizes the privacy framework and operating model for TTS-US

As the need arise, this Policy will be supplemented by additional policies, procedures, and guidelines, to address specific areas, jurisdictions, laws, and requirements.

TTS-US is committed to protecting the rights of individuals with regards to Processing of their Personal Information and acting in accordance with applicable laws and regulations.

TTS-US needs to Process Personal Information to carry out business and administrative activities and to provide products and services to its clients, customers, partners, and employees.

II. Scope

This Policy applies to all TTS-US's employees, agents, independent contractors, representatives, including any third-party provider of services to TTS-US ("**Third-Party Service Provider**") or those otherwise affiliated with TTS-US for the purposes of employment or provision of services who Process Personal Information TTS-US has collected or otherwise has in its possession. This Policy applies to all Personal Information collected, maintained, transmitted, stored, retained, or otherwise used by TTS-US regardless of the media on which that information is stored and whether relating to employees or any other person.

III. Definitions

1. "**Cyber Security Incident**" means an actual or suspected adverse event in an information system and/or network, or the threat of the occurrence of such an event. A Cyber Security Incident is a violation or imminent threat of violation of TTS-US computer security policies, acceptable use policies, or standard security practices. It implies harm or the attempt to harm.

2. "**Data Breach/Privacy Breach**" means the unauthorized access to and/or acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business. Data breaches also include the unauthorized access to and/or acquisition of physical documents. Good faith acquisition of personal information by an employee or agent of the person or business for the purposes of the person or business is not a breach of the security of the system, provided that the personal information is not used or subject to further unauthorized disclosure. The definition of a privacy-related data breach varies from state to state and changes regularly and must be analyzed during each Cyber Security Incident. The applicable state law is based on the current residency of each affected individual involved in the breach.

3. **"Data Subject"** means the person about whom Personal Information is being Processed.

4. **"Data Subject Rights"** means a range of rights, in the context of particular conditions that a Data Subject may exercise under Privacy legislation.

5. **"Personal Information"** means information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a natural person. Examples of Personal Information include, but are not limited to: names, addresses, phone numbers, and e-mail addresses.

6. "**Privacy Incident**" means any event that has resulted in (or could result in) unauthorized use or disclosure of PI/PHI where persons other than authorized Users have access (or potential access) to PI/PHI or use it for an unauthorized purpose.

7. **"Process" and "Processing"** means any operation or set of operations that are performed on Personal Information, including collecting, using, storing, accessing, modifying, transferring, recording, or deleting Personal Information.

8. **"Security Incident"** means any act or omission that compromises the security, confidentiality, or integrity of Personal Information or the physical, technical, administrative, or organizational safeguards TTS-US or a Third-Party Service Provider has put in place to protect Personal Information. The loss of or unauthorized access to, disclosure, or acquisition of Personal Information is a security incident.

9. **"Sensitive Personal Information"** means Personal Information collected, accessed, shared, used, or analyzed concerning a consumer's health, Personal Information collected and analyzed concerning a consumer's sex life or sexual orientation, or Personal Information that reveals:

- A consumer's social security, driver's license, state identification card, or passport number.
- A consumer's account log-in, financial account, debit card, or credit card number in combination with any required security or access code, password, or credentials allowing access to an account.
- A consumer's precise geolocation or inferences made from access to precise geolocation;
- A consumer's racial or ethnic origin, religious or philosophical beliefs, or union membership.
- The contents of a consumer's mail, email, and text messages unless the business is the intended recipient of the communication.
- A consumer's genetic data.
- The processing of biometric information for the purpose of uniquely identifying a consumer.
- Information otherwise defined by Privacy laws as "sensitive."

IV. Coordination and Responsibilities

A. TTS-US Privacy Program

TTS-US has established a Privacy Program, which is designed to develop, manage, and drive privacy initiatives. At a high level, the Privacy Program:

- Initiates and fosters a culture of privacy within TTS-US;
- Ensures that privacy is included in business objectives and goals;
- Ensure privacy training is provided to TTS-US; and
- Oversee compliance in a complex regulatory environment domestically and internationally.

The Privacy Program carries out the above with input from and collaboration with various functions within TTS-US, such as Legal, Information Technology, and Information Security.

B. **TAI Head of Privacy**

The Head of Privacy at Toyota Tsusho America ("TAI") provides oversight for TTS-US' Privacy Program.
TTS-US is accountable for initiation and implementation of its privacy objectives.

C. **Privacy Champion**

TTS-US will appoint a Privacy Champion(s) whose responsibility is to manage and maintain TTS-US' Privacy Program. These individuals shall cooperate and collaborate with TAI Head of Privacy with the implementation of TTS-US' Privacy Program.

D. **Board**

TAI's Head of Privacy shall report to the TTS-US board, at least once per year. An annual report shall be presented to TTS-US Board, or designated committee, summarizing significant events during the previous calendar year (e.g., milestones achieved).

V. Privacy Operating Model

TTS-US Privacy Program protection of Personal Information is tied to Toyota Tsusho Core Values and Toyota Tsusho Group Way.

VI. Privacy Principles

A. **General Principles Relating to the Processing of Personal Information**

TTS-US shall strive to ensure that the principles set forth in this Policy are taken into account (i) in the design and implementation of all procedures involving the processing of Personal Information; (ii) in the products and services offered thereby; (iii) in all contracts and obligations that they formalize with natural persons; and (iv) in the implementation of any systems and platforms that allow access by TTS-US professionals or third parties to Personal Information and the collection or processing of such information. The principles relating to the processing of Personal Information on which this Policy is based include:

TTS-US Privacy Principles
1. Accountability & Authority
2. Purpose Limitation
3. Transparency

1. Accountability & Authority. Each person or company who processes Personal Information is responsible to ensure that Personal Information is processed in a compliant manner, under the oversight of the TTS-US Privacy Program. Each person or company processing Personal Information must only create, collect, use, process, store, maintain, disseminate, or disclose Personal Information if they have authority to do so, and should identify this authority in the appropriate notice.

2. Purpose Limitation. Personal Information should be collected for specified, explicit, legitimate, and lawful purposes, and in a manner compatible with the purposes which the Personal Information was initially collected.

3. Transparency. Data Subjects should be informed about the creation, collection, use, processing, storage, maintenance, dissemination, and disclosure of Personal Information.

4. Data Minimization. Personal Information will be collected only where reasonable and necessary for the stated purposes for which it is being Processed, and will be adequate, relevant, and limited to what is necessary in relation to those purposes.

5. Storage Limitation. Personal Information should only be retained for as long as is necessary for the purpose for which it was obtained, except in the circumstances established by law. TTS-US will follow the applicable records retention schedules and policies and destroy any media containing Personal Information in accordance with the applicable Document Retention Policy.

6. Accuracy. Personal Information should be accurate and, if necessary, kept up to date. Reasonable steps will be taken to ensure the accuracy of Personal Information obtained.

7. Data Subject Rights. Data Subject Rights depends on local, regional, and country privacy laws and allow Data Subjects to request certain information and action regarding their information.

8. Security. Appropriate organizational, administrative, physical, and technical safeguards and procedures shall be implemented to protect the security of Personal Information, including against or from accidental or unauthorized destruction, loss, alteration, disclosure, access, or unplanned loss of availability.

B. **Jurisdictional Principles Relating to the Processing of Personal Information**

TTS-US shall comply with personal data protection laws in applicable jurisdictions, the laws that apply based on the processing of Personal Information that TTS-US carry out and the laws determined by binding rules or resolutions adopted within the TTS-US.

VII. Privacy Governance

A. **Privacy Control Management and Regulatory Requirements**

1. **Privacy Controls**
   Privacy controls are the administrative, technical, and physical safeguards employed within organizations to comply with applicable privacy laws and regulations and protect and ensure the proper handling of Personal Information.

   TTS-US shall create adequate controls to measure the efficiency of this Policy. TTS-US's privacy controls are loosely based on the NIST Special Publication 800-53 Rev. 5 and described in Section VII.

2. **Regulatory Requirements**
   Personal Information that requires TTS-US to implement specific privacy and security safeguards as mandated by federal, state, international, and/or local law, or TTS-US policy or agreement. Examples of regulations and categories include:
   - State privacy laws and regulation
   - 50 state notice of breach laws
   - Social Security Numbers (SSNs)
   - Industry mandated regulations, such as the Payment Card Industry Standards (PCI-DSS)

B. **Transparency and Privacy Notice**
TTS-US will notify Data Subjects of the Personal Information that it Processes about them as required by applicable data protections laws, including notice of the following: the types of Personal Information collected, the purposes of the Processing, Processing methods, the Data Subjects' rights with respect to their Personal Information, the retention period, potential international data transfers, if data will be shared with third parties and the TTS-US's security measures to protect Personal Information.

This information is contained in the TTS-US's Employee Privacy Policy.

C. **Privacy Training and Awareness**
TTS-US shall provide training and take appropriate action to raise awareness so as to ensure the effective implementation of this Policy by its personnel, considering resources and logistics constraints.

All TTS-US personnel who have access to Personal Information must be educated and trained on this Policy and the treatment of Personal Information at least annually.

TAI Head of Privacy, and the TTS-US Privacy Champion, is responsible for developing the training content. The TTS-US Privacy Champion is responsible for determining which individuals must receive the training required by this section and to ensure the documentation of the time, date, place, and content of each training session, as well as who attended each training sessions.

VIII. Privacy Impact and Risk Assessment

A. **Privacy Risks**
TTS-US Privacy Champion is responsible for documenting and implementing a Privacy Risk Management process once the Privacy Program is implemented and established.

B. **Privacy Impact Assessment (Privacy Questionnaire)**
Privacy Impact Assessment (PIA) is a process to help identify and minimize the data protection risks involved in projects, processes, and activities involving the processing of Personal Information. PIAs are required for processing likely to result in high risk to the individuals and their Personal Information, and where new technologies are involved. TTS-US requires a PIA for any projects involving the use of Sensitive Personal Information, including new systems, solutions, and some research studies.

IX. Personal Information Handling

A. Personal Information Lifecycle Management

TTS-US shall implement privacy considerations into the life cycle of Personal Information, programs, information systems, mission/business processes, and technology.

TTS-US shall incorporate privacy analysis into each stage of the data lifecycle (i.e., collection, use, retention, processing, disclosure, and destruction), from the early design stage to start up, use, and disposal.

B. Personal Information Inventory and Maps Process

TTS-US will maintain data inventory or data maps, including records as set forth in applicable data protection laws.

C. Policies/Procedures for Handling Personal Information

TTS-US shall process Personal Information only on one of the following bases:

a) in order to enter into or execute a contract with the Data Subject;

b) in order to apply its internal legislation and comply with its legal obligations;

c) in order to pursue its legitimate interest or for a business purpose as defined by applicable data protection laws, provided that this does not outweigh the privacy rights of the Data Subject as set out in this Policy;

d) where such processing is in the vital interest of the Data Subject;

e) where such processing is necessary for the purposes of maintaining the TTS-US's archives, for scientific or historical research or for the preparation of statistics, always subject to the relevant internal legislation and policies; or

f) with the Consent of the Data Subject.

D. Sensitive Personal Information Handling

The processing of Sensitive Personal Information shall be prohibited, except in the following situations:

a) such processing is necessary for TTS-US to carry out its legal obligations;

b) such processing is necessary for TTS-US to carry out internal investigations or disciplinary procedures, or in the settlement of disputes;

c) such processing is necessary for the establishment, exercise, or defense of legal claims;

d) such processing is necessary for the protection of the vital interests of the Data Subject or another person, and the Data Subject is legally or physically incapable of giving consent;

e) such processing is essential for carrying out TTS-US's business activities, business purposes, or legitimate interests provided that appropriate safeguards are implemented and that no less intrusive measures are reasonably available;

f) the Sensitive Personal Information has been manifestly made public by the Data Subject; or

g) the Data Subject Consents to such processing.

E. Securing Controls for Personal Information

TTS-US is required to take steps to ensure proper use of Personal Information. These steps include monitoring the use of Personal Information and training organizational personnel on the authorized uses of Personal Information.

F. Transfers

1. **Transfers Between Corporate Entities**
TTS-US may share Personal Information with its affiliates and subsidiaries only for the authorized purposes identified in a contract, the privacy notice(s) and/or privacy policy or in a manner compatible with those purposes and in compliance with applicable laws.

2. **Transfers Between TTS-US and Third Parties**
TTS-US may share Personal Information with third parties that provide services to TTS-US to the extent such third parties are contractually required to follow the procedures set forth herein, or substantially equivalent standards, and to protect Personal Information in accordance with all relevant laws, regulations, and rules, and subject to any appropriate security measures and directions from TTS-US. These requirements should also apply to any subcontractors engaged by third parties.

3. **Transfers Across Boarders**
TTS-US must take steps to ensure that cross-border transfers of Personal Information are subject to adequate safeguards. Personal Information that is transferred cross-border must be Processed by or on behalf of TTS-US in accordance with applicable data protection laws, and TTS-US policies and agreements.

X. Security

A. **Security of Personal Information**
TTS-US shall implement an Information Security Program (ISP) that sets forth technical, administrative, and physical safeguards for the protection of Personal Information. TTS-US shall exercise particular care in protecting Sensitive Personal Information from loss, unauthorized access, and unauthorized disclosure.

B. **Reporting Personal Information Security Incidents or Breaches**
In general, privacy laws in the jurisdictions where TTS-US operates require notification, in some circumstances, of Personal Information breaches to local authorities, and in certain instances, to the Data Subject whose Personal Information is involved in the incident. TTS-US has put in place procedures to deal with any suspected unauthorized access, processing, disclosure, or loss of Personal Information and will notify Data Subjects or any applicable regulator where the company is legally required to do so.
If a TTS-US employee becomes aware of an unauthorized access, processing, disclosure or loss of Personal Information, such employee must not attempt to investigate the matter him/herself and must instead contact the person identified in the Incident Response Policy. Please refer to TTS-US's Incident Response Policy for specific protocols.

C. **Privacy Incident Regulatory Requirements**
Incidents involving Personal Information should be reported to the contact noted in the Incident Response Policy and in TTS-US CSIRP.
TTS-US Privacy Champions shall report incidents in the manner documented in TTS-US' CSIRP.

XI. Data Subject Rights and Requests

A. **Procedure for Data Request Handling**
State and country laws grant Data Subjects with specific and varying rights related to their Personal Information and how it is Processed. Most laws grant Data Subjects the right to request access to their Personal Information, the right to request that their Personal Information be corrected, the right to request that the processing of their Personal Information is stopped or cancelled and the right to object to the processing of their Personal Information.

TTS-US shall establish a procedure for responding to requests from Data Subjects based on their legal rights, as detailed in the Data Subject Access Request Policy.

XII. Privacy Third Party Oversight

A. **Privacy Vendor Management Procedure**
Vendors and other third parties must be assessed, engaged, and managed in accordance with applicable law.

B. **Privacy Requirements for Third-Party Service Providers**
Third-Party Service Providers that Process Personal Information may only be engaged if they are capable of meeting adequate standards and providing appropriate safeguards for Personal Information. At a minimum:

- Appropriate due diligence should be conducted of Third-Party Service Providers who process Personal Information and Sensitive Personal Information
- Appropriate contractual obligations must be implemented with each Third-Party Service Providers, which include (where relevant) contractual obligations that are equivalent to those which apply to TTS-US under applicable data protection laws.

XIII. Non-Compliance

Any employee or contractor who violate this policy may be subject to discipline, per rules of conduct as noted in the Employee Handbook.

XIV. Related Policies

Other TTS-US policies also apply to the collection, use, storage, protection, and handling of Personal Information and may be relevant to implementing this Policy. You should familiarize yourself with these policies, including:

- Acceptable Use Policy.
- TTS-US Employee Privacy Notice.
- Data Subject Rights Policy
- Incident Response Policy

XV. Disclaimer of Restrictions on Employees' Rights

This Policy is not intended to restrict communications or actions protected or required by state or federal law.

XVI. Amendment and Revision

This Policy may be revised from time to time.

XVII. Authorization and Revision History

A. **Authorization**

Authorized by:	Norihito Ohigashi	**Signature:**	
Title:	President and CEO	**Date**:	

[ここに入力]

B. **Revision History**

Rev. No.	Date	Description of Revision	Revised Page(s)	Approved by:
1.0	08/22/2024	Initial Version	NA	TTS-US BOD