

Data Processing Agreement (DPA)

This Data Processing Agreement ("Agreement") is entered into by and between:

Controller: [Client Name] (the "Data Controller")

Processor: Skynet Technologies USA LLC (the "Data Processor")

Effective Date: [Insert Date]

1. Definitions

For the purposes of this Agreement:

- **"Personal Data"** means any information relating to an identified or identifiable natural person.
 - **"Processing"** means any operation performed on Personal Data, such as collection, storage, use, disclosure, or deletion.
 - **"Sub-processor"** means any third party engaged by the Processor to process Personal Data.
 - **"Data Protection Laws"** means applicable laws including the EU GDPR, UK GDPR, Swiss FADP, CCPA/CPRA, and other relevant privacy regulations.
 - **"Services"** means the provision of the *All in One Accessibility* solution by Skynet Technologies.
-

2. Subject Matter and Duration

This Agreement governs the Processing of Personal Data by the Processor on behalf of the Controller in connection with the provision of the Services. The Agreement remains in effect for as long as the Processor processes Personal Data on behalf of the Controller.

3. Nature and Purpose of Processing

The Processor shall process Personal Data solely for the purpose of:

- Account registration and login management.
- User session management.



SKYNET TECHNOLOGIES



- Accessibility settings preferences.
 - Customer support and technical assistance.
 - Service improvements, troubleshooting, and analytics (non-identifiable where possible).
-

4. Types of Personal Data

Personal Data processed may include, but is not limited to:

- Full name.
 - Email address.
 - Login method (Google, Microsoft, Apple, or email/password).
 - Login timestamps.
 - Customer support communications.
 - Technical identifiers such as IP address, device type, and browser information.
-

5. Categories of Data Subjects

The categories of Data Subjects include:

- End users of the All in One Accessibility solution.
 - Customers authorized to manage their widget settings.
 - Support contacts interacting with Skynet Technologies.
-

6. Obligations of the Data Processor

The Processor shall:

1. **Instructions** – Process Personal Data only on documented instructions from the Controller.
2. **Confidentiality** – Ensure all persons authorized to process Personal Data are bound by confidentiality obligations.



SKYNET TECHNOLOGIES



3. **Security** – Implement appropriate technical and organizational measures to protect Personal Data (see Annex II).
 4. **Assistance** – Assist the Controller in responding to data subject rights requests.
 5. **Breach Notification** – Notify the Controller without undue delay, and no later than **72 hours**, upon becoming aware of a Personal Data Breach.
 6. **Data Deletion/Return** – At the end of services, delete or return all Personal Data unless retention is required by law.
 7. **Records** – Maintain records of Processing activities as required by law.
-

7. Sub-processors

The Controller agrees that the Processor may engage sub-processors to fulfil its obligations, provided that:

- The sub-processor is contractually bound to data protection obligations no less protective than those in this Agreement
- The Processor shall remain fully liable for the acts and omissions of its sub-processors

Annex I – Current Sub-processors lists all approved sub-processors.

8. International Data Transfers

Any transfer of Personal Data to a third country outside the EEA, UK, or Switzerland shall be subject to appropriate safeguards such as **Standard Contractual Clauses (SCCs)**, the **EU-U.S. Data Privacy Framework**, the **UK Extension**, or the **Swiss-U.S. Data Privacy Framework**, as applicable.

9. Security Measures

The Processor applies a layered security program including, but not limited to:

- Data encryption in transit (TLS) and at rest.
- Strong access controls and 2FA.
- Regular backups and disaster recovery planning.

- Staff training on data protection and security.

Details are provided in Annex II – Security Measures.

11. Data Subject Rights

The Processor shall assist the Controller by appropriate technical and organizational measures, insofar as possible, in fulfilling the Controller’s obligation to respond to requests from Data Subjects (e.g., access, correction, erasure, portability, objection).

12. Termination

Upon termination of the Services, the Processor shall, at the Controller’s choice:

- Delete all Personal Data, or
- Return all Personal Data in a commonly used format.

The Processor will confirm deletion in writing, unless retention is required by law.

13. Governing Law

This Agreement is governed by and construed in accordance with the laws of the State of Kentucky, United States, unless otherwise required by applicable Data Protection Laws.

Annex I – Current Sub-processors

Sub-processor	Description	Regions
InMotion Hosting	Infrastructure hosting and storage	• US – Los Angeles, CA • US – Ashburn, VA • Europe – Amsterdam For more details click here
SMTP2GO	Customer communication email	• USA • Europe



SKYNET TECHNOLOGIES



	service	Australia For more details click here
Cloudflare	Content delivery network (CDN) and web security	Global – North America, Europe, Asia, Africa, Middle East (100+ locations worldwide) For more details click here
Stripe	Payment processing services	United States (Colorado – Denver), Global (supported in 50+ countries) For more details click here
PayPal	Payment processing services	United States (Arizona – Scottsdale & Phoenix, California – San Jose), Global (multiple countries)
Google Cloud	Text-to-Speech (TTS) and AI services	United States, Europe (Netherlands, Germany, UK, Finland), Asia (Singapore, Taiwan, India, Japan), Australia, South America (Brazil), Middle East (Israel, Saudi Arabia), Africa (South Africa) For more details click here
Microsoft Azure	Text-to-Speech (TTS) and AI services	United States, Europe (Ireland, Netherlands, UK, France, Germany), Asia (India, Japan, China, Korea, Southeast Asia), Australia, South America (Brazil), Middle East (Qatar, UAE), Africa (South Africa) For more details click here

Annex II – Security Measures

Skynet Technologies implements the following security measures:

1. Organizational Security

- Designated Data Protection Officer (DPO).
- Staff confidentiality agreements.
- Regular data protection and security training.

2. Technical Security

- TLS encryption for all data in transit.
- AES-256 encryption for stored data.
- Role-based access with least-privilege principle.
- Multi-factor authentication (MFA).
- Regular vulnerability scanning and penetration testing.

3. Operational Security

- Daily system monitoring and log review.
- Intrusion detection and prevention systems.
- Regular backups with secure storage.
- Business continuity and disaster recovery planning.

IN WITNESS WHEREOF, the parties hereto have executed this Data Processing Agreement as of the Effective Date.

For Controller (Client)

For Processor (Skynet Technologies USA LLC)