Policy on the Protection of Privacy and Personal Data

Universal Scientific Industrial (Shanghai) Co., Ltd. ("**Company**"), as a subsidiary of ASE Technology Holding Co., Ltd., values the importance of privacy and personal data protection. This **Policy on the Protection of Privacy and Personal Data** (the **"Policy**") is adopted by Company in accordance with the Personal Data Protection Act of Taiwan, Enforcement Rules of the Personal Data Protection Act of Taiwan, EU General Data Protection Regulation (GDPR) and applicable laws and regulations on the protection of privacy and personal data in the United States (U.S.), China and other countries or areas where Company or its affiliates (collectively "**USI**") operate, to guide and manage the compliance by USI. The Policy aims to protect the personal data ("**Personal Data**") of USI's customers and suppliers, visitors, website users, investors or shareholders, job applicants and employees ("**data subject**"). USI hereby commits to collect, process and use Personal Data in strict accordance with the Policy and requesting each of USI's suppliers (including vendors, contractors, external consultants) to implement relevant compliance management in compliance with the Policy, cooperate with USI to protect the privacy and personal data, and secure the rights and interests of data subject.

A. Purpose of Collection, Processing and Use

USI may collect, process and use personal data for the following purposes ("**Specific Purpose**"):

1. **Business operation:** via email or through other channels, to perform works, cooperate or communicate, negotiate or fulfill contracts, etc.
2. **Commercial marketing:** via email, website or through other channels, to provide business information or cooperation channels relevant to USI, or respond to or communicate related matters.
3. **Security management:** through appropriate measures to ensure the security of data, personnel and the facility.
4. **Website maintenance and communication:** to improve the function and services of the company's website, provide the latest information related to business and investment, or respond to website user's inquiries.
5. **Recruitment and job applicant interviews, employee management and providing services to the employees**
6. **Where it is necessary to fulfill statutory obligations**
7. **Where it is necessary to assist public authorities in performing statutory duties:** such as investigation of illegal activities, prevention or investigation of criminal cases
8. **Where it is necessary to assert, exercise or protect USI's legal rights**
9. **To conduct various operational management procedures**

B. Collection, Processing and Use of Personal Data

I. Under specific circumstances, USI may collect, process and use certain personal data as follows:

1. USI may collect, process and use the personal data of personnel communicating, collaborating or conducting any interaction with USI in the course of business-related functions through meetings, activities or other business channels, as follows:

   - Personal information identifiers, including name, gender, employer and business title
   - Contact information including telephone number and e-mail address
   - Other information that may be used to directly or indirectly identify the personnel

2. To ensure the safety and security of both the personnel and workplace environment, USI may collect, process and use the personal data of persons entering USI facilities for the purpose of performing job duties or business visits, as follows:

   - Personal information including name, gender, employer, business title, ID/passport number or other forms of identification and facial photography.
   - Contact information including correspondence address, telephone number and e-mail address
   - Other information necessary for furthering public interests

3. For the purpose of employee management and the provision of services to the employees, USI may collect, process and use the Personal Data of the employees when they participate in the daily operation of USI, as follows:

   - Personal information identifiers, including name, gender, birth date, ID /passport number or other forms of identification and facial photography, etc.
   - Expertise and experience, including educational background, language ability and other professional skills or qualification certificates
   - Contact information including correspondence address, telephone number and e-mail address
   - Other information that may be used to directly or indirectly identify the employee
   - Other information necessary for furthering public interests

4. USI may collect, process and use the personal data of persons visiting the company's website and utilizing the web services to interact with Company (such as subscription to USI News Letter, online inquiries and use of other online systems), as follows:

   - Personal information including name, gender, employer, business title
   - Contact information including correspondence address, telephone number and e-mail address
   - Other information that may be used to directly or indirectly identify the website user, such as website user's relation with Company
   - Data collected by Cookies

5. USI may collect, process and use the personal data of individuals making investment enquiries about the Company through phone, e-mail or any communication

channels or persons who become shareholders of the Company, as follows:

- Personal information, including name, gender, employer, business title, ID/passport number or other forms of identification and facial photography
- Contact information, including correspondence address, telephone number and e-mail address
- Other information that may be used to directly or indirectly identify them

6. USI may collect, process and use the personal data of job applicants for vacant positions at USI, as follows:

- Personal information, including name, gender, birth date, ID /passport number or other forms of identification and facial photography.
- Expertise and experience, including educational background and occupation, language ability and other professional skills or qualification certificates
- Contact information, including correspondence address, telephone number and e-mail address
- Other information that may be used to directly or indirectly identify the job applicant
- Other information necessary for furthering public interests

II. USI shall not collect, process and use sensitive personal data including medical records, healthcare, physical examination and criminal records except for the following situations:

1. Where it is expressly required by applicable laws and regulations
2. Where it is necessary to fulfill statutory obligations with maintenance and protection measures that are appropriate and secure
3. Where it is necessary to assist the public authority in performing its statutory duties of investigating illegal activities, preventing or investigating criminal cases
4. Consent is given by the data subject

III. Unless notification may be waived in accordance with the applicable laws and regulations, USI shall inform the data subject of the followings:

1. Specific Purpose for the collection, processing and use of personal data
2. Data subject may decide to consent or reject USI's collection, processing and use of requested or suggested personal data **(opt-in)**
3. If data subject rejects to provide the Personal Data or if the Personal Data provided is inaccurate, USI may not be able to provide the data subject with specific or complete information, feedback or services, or complete recruitment processes or other employment management matters.

IV. USI shall collect, process and use personal data to the extent not exceeding the necessary scope of Specific Purpose and ensure the collection, processing and use of personal data that have legitimate and reasonable connection with Specific Purpose. The data subject may request the cessation of the collection, processing and use of personal data by USI, or deletion/destruction of personal data collected, processed or used by USI **(opt-out)** and USI shall proceed in accordance with such request (subject to certain exceptions, including the exceptions set forth in Section H). To exercise rights

over personal data, submit a request to the contact information provided in Sub-Section V of Section I. USI may need to validate the request. In order to validate a request, USI may ask for the following information: [name, prior interactions with USI, the name of the relevant company or business partner, corporate email address, or OTHERS]. Only the data subject or an authorized agent may make a request related to personal data. To designate an authorized agent, please provide a legally binding written document signed by the data subject and the identifying agent. USI may also verify the identity of the authorized agent.

V. If you are a California resident, for more information about USI's collection, processing, and use of personal data pursuant to the California Consumer Privacy Act (CCPA), please refer to Addendum "A".

C. Third Party Disclosure

I. USI may disclose personal data to third parties under the following circumstances:

1. The third party is a public authority:

- Where it is necessary to fulfill statutory obligation
- Where it is necessary to assist the public authority (the Court, Prosecutor/Policy/Investigation Bureau, or national or local government agency, etc.) in performing its statutory duties of investigating illegal activities, preventing or investigating criminal cases
- Where it is necessary to assert, exercise or protect USI's legal rights
- At the request of the data subject

2. The third party is a private legal entity (including Company's affiliates), private institution or organization, or individual persons:

- Where it is necessary to fulfill statutory obligation
- Where it is necessary to assert, exercise or protect USI's legal rights
- For business or commercial use to the extent not exceeding the necessary scope of the Specific Purpose
- At the request of the data subject

II. USI shall manage third party disclosures in compliance with the following:

1. Verifying the identity of the third party
2. Notifying data subject and obtaining his/her consent unless notification may be waived in accordance with applicable laws and regulations (e.g. notification or consent may prevent the public authority from performing statutory duties)
3. Disclosing minimal and only necessary personal data, and requiring third parties to comply with applicable laws and regulations on personal data protection

III. For more information about USI's Third Party Disclosures pursuant to the CCPA, please refer to Addendum "A".

D. Accuracy of Personal Data

USI shall take measures that are reasonable and necessary to maintain the accuracy of personal data and, proactively or at the request of the data subject, supplement or correct personal data.

E. Retention and Security of Personal Data

I. USI shall retain Personal Data for a reasonable period of time not exceeding the necessary scope of Specific Purpose, which in principle does not exceed 5 years (or for the Personal Data of the employees, not exceeding 5 years following the termination of the employment). Unless continuous retention of personal data is expressly required by applicable laws and regulations or necessary for USI to perform duties or business, or has the consent of the data subject, USI shall, proactively or at the request of the data subject, cease the collection, processing and use of personal data, or delete/destruct personal data if collection, processing and use is no longer necessary, the legitimate and reasonable connection with Specific Purpose no longer exists, or the laws and regulations on retention become not applicable.

II. USI shall establish appropriate and secure measures to manage the storage, processing, transmission, retention, access privileges of personal data and data storage/transfer tools. USI shall commit to safeguarding personal data to prevent damage, loss, theft, leakage, unauthorized access, copies, use or alteration. The measures include:

1. Using appropriate and secure networks and tools for data transmission and storage, such as encryption software (SSL or HTTP) to transfer data and setting up firewalls
2. Classifying personal data according to level of security to ensure that the collection, processing and use of such data do not exceed the necessary scope of the Specific Purpose, and preventing access by unauthorized personnel.
3. Classifying personal data according to results of risk assessments, and adopting appropriate management procedures for the collection, processing, use and disclosure of such data.

F. Cross-Border Transfer

Personal data may be transferred among and used by Company's affiliates located in different countries to the extent not exceeding the original scope of the Specific Purpose. USI shall manage the transfer and use of personal data in accordance with the Policy and applicable privacy and personal data laws and regulations in the countries where the personal data is transferred and used.

G. Website Cookies

To improve and enhance the company's website services, USI uses cookies to collect, process and use certain persona data, such as the user's internet protocol address. To know more about our use of cookies, please refer to USI's Cookie Terms.

H. Legal Rights

With respect to personal data collected, processed and used by USI, the data subject may be entitled to the legal rights as follows:

1. The right to request an inquiry or review
2. The right to request a copy
3. The right to supplement or correct the incomplete or incorrect personal data
4. The right to request the cessation of collection, processing and use (in terms of Personal Data of the employees, USI may still maintain the Personal Data necessary for its daily operation, management and provision of services based on its internal policies, but USI shall comply with the relevant requirements under the Policy for such retained Personal Data)
5. The right to request the deletion/destruction of personal data that is displayed or stored internally at USI, or publicly available on public websites, files or other forms of storage
6. Where necessary and technically feasible, the right to request the transfer of personal data, in electronic and machine readable format, to designated third party data controller
7. The right to report any personal data violation to public authorities in the area where the data subject is a resident or where the personal data is used

USI does not sell or share (as those terms are defined under the CCPA) personal data.

USI does not disclose or use sensitive personal data outside of the permissible uses identified within the CCPA.

USI will not discriminate against a data subject for exercising legal rights.

To request an appeal of any decisions made by USI regarding exercising Legal Rights over personal data, contact USI at privacy@usiglobal.com.

I. Others

I. The protection of privacy and personal data is an integral component of USI's internal control and risk management system. On an annual basis, the USI conducts risk assessments and internal compliance audits. From to time to time, USI also conducts supplier compliance audits and engages independent parties to audit USI's implementation of privacy and personal data protection to ensure full compliance with Policy and applicable laws and regulations.

II. USI's new employees are required to complete a training course on the protection of privacy and personal data. All employees of USI also receive regular updates on relevant laws and regulations governing privacy and personal data and management guidance to enhance their compliance awareness.

III. USI adopts a zero-tolerance policy to any violation of privacy and personal data

protection. Should a violation be identified after thorough investigations, USI shall immediately review and improve management measures, and take disciplinary actions against errant personnel and where necessary, seek indemnity or prosecution in accordance with applicable laws and regulations.

IV. USI's employees, external parties or natural persons may report violations, suspected violations or conducts that could result in a violation of the protection of privacy or Personal Data by submitting relevant materials through any channel most recently announced by the website of Company.

V. For matters concerning the Policy or any other issues related to privacy and personal data, USI's employees, external parties or natural persons may contact the following responsible department of USI:

Universal Scientific Industrial (Shanghai) Co., Ltd.
Legal, Compliance & IP Unit
+866 49 2350876
privacy@usiglobal.com

This Policy may be updated from time to time. Please refer to Company's website for the latest version. (This version was last updated on December 30, 2022.)

Frequently Asked Questions (FAQ)

Q1: What is personal data?

A: Personal data is information that in general may be used to identify a natural person such as name, birth date, ID/passport number, identifiable features, fingerprints, marital status, family information, educational background, occupation, contact information, financial status, and may include additional data on medical and healthcare records, genetics, social and physiological identity, records of physical examinations, criminal records, etc.

Q2: Why does USI need to use my personal? What/How my personal may be used?

A: Based on the types of your interaction with USI, USI may, for specific purposes, use certain information that may be used to identify you.
Please refer to Section A and Section B for a complete description of how your personal data may be used.

Q3: Can I refuse to provide my personal data?

A: You may decide to consent or refuse to provide personal data. However, refusal to provide or providing inaccurate or incomplete personal data may result in USI's inability to provide you with specific or complete information, feedback or services.
Please refer to Sub-Section III of Section B for more details.

Q4: Can I make request for my personal data?

A: You have a legal right to request USI to stop collecting, processing and using your personal data, or delete/destruct your personal data and related records.

Please refer to Sub-Section IV of Section B and Section H for more details.

Q5: How do I contact USI to make enquiries on personal data?

A: You may contact our Legal, Compliance & IP Unit at +866 49 2350876 or email privacy@usiglobal.com

Please refer to Section IV and V of Section I of Policy

Q6: Can I appeal any decisions made by USI regarding my legal rights over my personal data?

A: You may have a right to appeal decisions made by USI regarding your legal rights over your personal data.

Please refer to Section H for more details.

TITLE	**ADDENDUM "A" -** UPPLEMENTAL PRIVACY NOTICE FOR CALIFORNIA CONSUMERS
INFO	

This Supplemental Privacy Notice for California Consumers ("**Notice**") supplements the Policy on the Protection of Privacy and Personal Data ("**Policy**") and applies solely to USI's customers and suppliers, visitors, website users, investors or shareholders, job applicants and employees residing in California. USI adopts this Notice to comply with the California Consumer Privacy Act (CCPA), and any amendments and implementing regulations, and any terms defined in the CCPA have the same meaning when used in this Notice.

Categories of Personal Information USI Collects

Over the last twelve (12) months, USI has collected the following categories of personal information from customers and suppliers, visitors, website users, investors or shareholders, job applicants and employees:

Category	Examples	Collected	Third Parties Shared
A. Identifiers.	A real name, alias, postal address, unique personal identifier, online identifier, Internet Protocol address, email address, account name, Social Security number, driver's license number, passport number, or other similar identifiers.	For all data subjects, where applicable. For website users, only name, country-location, and email address are collected.	(a) Human resources information service providers (b) Financial investment service providers (c) General Affairs program service providers (d) Insurance providers (e) Payroll service providers (f) Physical security vendors
B. Personal information categories listed in the California Customer Records statute (Cal. Civ. Code § 1798.80(e)).	A name, signature, Social Security number, physical characteristics or description, address, telephone number, passport number, driver's license or state identification card number, insurance policy number, education, employment, employment history, bank account number, credit card number,	For all data subjects, where applicable. For website users, only name, country-location, and email address are collected.	(a) Human resources information service providers (b) Financial investment service providers (c) General Affairs program service providers (d) Insurance providers (e) Payroll service providers (f) Physical security

		debit card number, or any other financial information, medical information, or health insurance information.		vendors
	C. Protected classification characteristics under California or federal law.	Age (40 years or older), race, color, ancestry, national origin, citizenship, religion or creed, marital status, medical condition, physical or mental disability, sex (including gender, gender identity, gender expression, pregnancy or childbirth and related medical conditions), veteran or military status, genetic information (including familial genetic information).	For all job applicants and employees.	(a) Human resources information service providers (b) Financial investment service providers (c) General Affairs program service providers (d) Insurance providers (e) Payroll service providers (f) Physical security vendors
	D. Commercial information.	Records of products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.	For customers and suppliers, visitors, investors or shareholders.	(a) General Affairs program service providers
	E. Biometric information.	Genetic, physiological, behavioral, and biological characteristics, or activity patterns used to extract a template or other identifier or identifying information, such as, fingerprints, faceprints, and voiceprints, iris or retina scans, keystroke, gait, or other physical patterns, and sleep, health, or exercise data.	For all data subjects.	(a) Physical security vendors
	F. Internet or other similar network activity.	Browsing history, search history, information on a consumer's interaction with a website,	For all data subjects.	(a) Cybersecurity vendors

	application, or advertisement.		
G. Professional or employment-related information.	Current or past job history or performance evaluations.	For job applicants and employees.	(a) Human resources information service providers
H. Non-public education information (per the Family Educational Rights and Privacy Act (20 U.S.C. Section 1232g, 34 C.F.R. Part 99)).	Education records directly related to a student maintained by an educational institution or party acting on its behalf, such as grades, transcripts, class lists, student schedules, student identification codes, student financial information, or student disciplinary records.	For job applicants and employees.	(a) Human resources information service providers
I. Sensitive personal information	Personal information that reveals government IDs; information providing access to a financial account; racial or ethnic origin; personal information collected and analyzed concerning an employee's health.	For job applicants, employees, investors or shareholders, however, information is collected and used consistent with the permissible uses under the CCPA.	(a) Human resources information service providers (b) Financial investment service providers (c) Government entities or regulators