KULICKE & SOFFA (SUZHOU) LIMITED

ASSEMBLEON TECHNOLOGY (SUZHOU) CO., LTD.

KULICKE & SOFFA (SHANGHAI) INTERNATIONAL TRADING CO., LTD.

GLOBAL DATA PROTECTION POLICY – CHINA ADDENDUM/POLICY

GLOBAL DATA PROTECTION POLICY - CHINA ADDENDUM/POLICY

Kulicke & Soffa (Suzhou) Limited
Assembleon Technology (Suzhou) Co., Ltd.
Kulicke & Soffa (Shanghai) international Trading Co., Ltd.

(collectively referred to as the "**Organization**")

1. INTRODUCTION

1.1 Background To China's Personal Data Protection Framework

1.1.1 Legal framework

(a) Cybersecurity Law of the People's Republic of China (the "**Cybersecurity Law**", in Chinese 网络安全法), effective 1 June 2017, safeguards the rights of Individuals by imposing requirements on network operators who collect and process Personal Data.

(b) Civil Code of the People's Republic of China (the "**Civil Code**", in Chinese 民法典), effective 1 January 2021, safeguards the rights of Individual by imposing requirements on personal data processors that collect and process Personal Data.

(c) Information Security Technology – Personal Information Security Specification (the "**Specification**", in Chinese 个人信息安全规范, together with Cybersecurity Law and Civil Code, the "**China Applicable Regulations**"), as amended and effective 1 October 2020, provides detailed guidelines for network operators to protect Personal Data under the Cybersecurity Law.

(d) The foregoing laws and standards are applicable to the Organization and the Organization is committed to complying with them.

1.1.2 Administrative authorities. China's Personal Data protection framework is administered by four major authorities: the Cyberspace Administration of China, the Ministry of Public Security ("**MPS**"), the Ministry of Industry and Information Technology, and the State Administration for Market Regulation. MPS is the primary contact for reporting leaks of Personal Data.

1.2 Background to China Addendum/Policy

1.2.1 This China Addendum/Policy (this "**China Policy**") supplements the global data protection policy (the "**Global Data Protection Policy**") of Kulicke and Soffa Industries, Inc. and/or any of its affiliates (collectively, "**K&S**") and should be read together as one policy. Save as set out in this China Policy, all other terms and principles in the Global Data Protection Policy shall continue to apply. This China Policy shall apply to all K&S entities incorporated in China and all processing of Personal Data by K&S in China.

1.2.2 This China Policy shall prevail in the event of inconsistency between the principles or contents stated herein and those as described under the Global Data Protection Policy.

1.3 China Addendum/Policy Part Of Employment Contract

1.3.1 All employees and agents of the Organization must strictly comply with this China Policy. For employees of the Organization, this China Policy binds each employee and forms a part of the terms of the employment contract between the Organization and the employee.

1.3.2 The Organization reserves its right to amend this China Policy from time to time. Any such amended China Policy will similarly apply to you and become part of your employment contract with the Organization from the time of such amendment taking effect.

1.3.3 This China Policy seeks to provide each employee with a broad summary overview of the requirements of the China Applicable Regulations and an understanding of the impact of the China Applicable Regulations on operational activities. For detailed information on the obligations and exceptions under the China Applicable Regulations, you may refer to the China Applicable Regulations themselves as well as guidelines [1] from the Cyberspace Administration of China and the State Administration for Market Regulation.

1.4 What To Do If You Are Aware Of Or Suspect A Breach of The China Applicable Regulations

1.4.1 If you have information or become aware that a breach under this China Policy, Global Data Protection Policy or otherwise under the China Applicable Regulations has occurred within the Organization, please report it immediately to the Data Protection Officer.

2. OVERVIEW OF THE CHINA APPLICABLE REGULATIONS

2.1 The Data Protection Obligations Applicable To Personal Data

2.1.1 With regard to dealing with Personal Data of any Individuals, the Organization and all employees are required to adhere to the following key **data protection principles/obligations**:

(a) Consent

(b) Purpose Limitation

(c) Minimum Necessity

(d) Rights of Individuals

(e) Protection and Security of Personal Data

(f) Transfer Limitation

(g) Notification

(h) Data Protection Officer

(The above data protection principles/obligations may be referred to in this document as the "**data protection principles**")

3. CONSENT

3.1 Introduction

3.1.1 Under the China Applicable Regulations, the Organization must obtain the consent of the Individual for the collection and processing (including but not limited to store, use, share, transfer or disclosure) of his or her Personal Data for any purpose, and such consent must be obtained prior to such collection and processing, unless an exception to the requirement of consent applies.

[1] Please find the full text of relevant guidelines Information as below:
(a) Information Security Technology-Guidance For Personal Information Security Impact Assessment (in Chinese, 信息安全技术-个人信息安全影响评估指南);
(b) Provisions on the Cyber Protection of Children's Personal Information (in Chinese, 儿童个人信息网络保护规定);
(c) National Emergency Response Plan for Cybersecurity Incidents (in Chinese, 国家网络安全事件应急预案).

3.2 Explicit Consent And Deemed Consent

3.2.1 Consent may be explicit or deemed.

3.2.2 As far as possible, explicit consent should be obtained. Check with the Data Protection Officer or the Organization's management if you are seeking to obtain consent other than by explicit means.

3.2.3 You should obtain consent in writing by using the issued form(s) and wording(s) approved and provided by the Organization's management. Do not use form(s) or wording that have not been approved by the Data Protection Officer or the Organization's management.

3.2.4 Personal Data of minors, individuals under the age of 18, are subject to different consent requirements. Before collecting Personal Data of minors aged 14 or older, you are required to obtain explicit consent from the minors or their guardians; where the minors are aged under the age of 14, you are required to obtain explicit consent from their guardians.

3.2.5 In dealing with the consent principle and the purpose limitation principle (elaborated below), the Organization has undertaken various compliance measures. These include but are not limited to (where relevant):

(a) ensuring that Individuals are notified of purposes for which their Personal Data may be processed by the Organization, method, scope of such data process and their respective consents obtained (in some cases such as CCTV signages (where relevant), the Organization will rely on the deemed consent concept);

(b) amending forms/documents where necessary;

(c) amending terms and conditions governing the customer relationship and/or the Organization's relationship with data intermediaries and other business partners, to deal with the China Applicable Regulations;

(d) amending the human resource related documents such as employment contract terms; and/or

(e) CCTV signage notification.

3.2.6 Ensure that you now deploy and use materials and processes, such as those above, which have been created or modified, in conformity with the China Applicable Regulations.

3.3 Consent As A Result Of False Or Misleading Information

Take note that consent will be invalid where it is given as a result of false or misleading information or has been obtained through deceptive or misleading practices. Thus all employees will need to ensure that they do not misrepresent, mislead or provide false information whenever consent is being obtained from Individuals.

3.4 Obtaining Personal Data From Third Parties

In many situations, the Organization will/may be collecting Personal Data from third parties other than the Individual himself (these third parties could be corporations or Individuals). In these situations, no such collection should be undertaken unless the following are satisfied:

(a) the third party has explained the source of such Personal Data to the Organization;

(b) the third party providing the Personal Data of Individuals has obtained the consent of those Individuals to disclose their Personal Data to the Organization for the specified purpose(s);

(c) those Individuals have indeed consented to the Organization collecting, using and disclosing their Personal Data for the specified purpose(s).

Please consult the Data Protection Officer if you have questions relating to this Section 3.4.

3.5 Exceptions To the Consent Requirement

3.5.1 The Organization may collect, or process Personal Data without an Individual's consent in limited circumstances as follows:

(a) where the collection or processing is in relation to Organization's performance of obligations specified in laws and regulations;

(b) where the collection or processing is in direct relation to State security or national defense security;

(c) where the collection or processing is in direct relation to public security, public sanitation, or major public benefits;

(d) where the collection or processing is in direct relation to investigations into crimes, prosecutions, court trials, execution of rulings, etc.;

(e) where the collection or processing is for purposes of safeguarding significant legal rights and interests, such as life and property, of the Individual or others, but it is difficult to obtain consent;

(f) where the Personal Data collected is the information voluntarily published by the Individual before the general public;

(g) where collecting or processing Personal Data is essential to the execution and performance of a contract requested by the Individual;

(h) where Personal Data is collected from information that has been legally and publicly disclosed, such as legal news reports and information published by the government; or

(i) where the collection or processing is necessary for ensuring the safe and stable operation of its products or services, such as identifying and disposing of faults in its products or services.

3.5.2 Note that relying on an exception does not exempt the Organization from having to comply with the remaining data protection principles as such an exception is only an exception to the consent and purpose limitation principles.

3.6 Withdrawal Of Consent

3.6.1 An Individual is entitled to withdraw his or her consent for the Organization to process his or her Personal Data at any time. An Individual who has previously consented to the collection, use or disclosure of his or her Personal Data for notified purposes can withdraw his or her consent at any time upon giving reasonable notice.

3.6.2 The Organization, or you, cannot prohibit an Individual from withdrawing his or her consent. Upon receipt of a notice of withdrawal from an Individual, which can come in any form such as an email, a letter, verbal notification etc. to any employee or representative of the Organization, the Organization should deal with the consent withdrawal request within 30 days.

3.6.3 You must not ignore any communication from an Individual wherein the Individual seeks to withdraw his or her consent. Immediately notify the Data Protection Officer and the Organization's management should you receive a request for withdrawal of consent.

3.6.4 Once the consent has been withdrawn, the Organization or you must no longer process the Personal Data concerned thereafter.

4. PURPOSE LIMITATION

4.1 Introduction

Under the China Applicable Regulations, the Organization must process the Personal Data that it collects in a manner consistent with the services it provides and in conformity with the agreement between the Organization and the Individual.

4.2 Clear Purpose

The Organization must have an unequivocal, clear and specific purpose in processing Personal Data.

4.3 Explicit Consent Required For Out-of-Scope Use

Where the Organization must process Personal Data beyond the original purpose, it must again obtain explicit consent of the Individuals affected.

5. MINIMUM NECESSITY

5.1 Introduction

Under the China Applicable Regulations, the Organization must collect Personal Data from Individuals only to the minimum extent necessary to achieve the purposes of collection, and continue to observe this minimum necessity principle in any subsequent data processing, use, storage, sharing, transfer and disclosure activities.

5.2 Necessary Type And Minimum Amount Of Personal Data

5.2.1 Only the necessary type and minimum amount of Personal Data required to support the purpose for which it was collected should be processed.

5.2.2 "**Necessary type**" refers to the type of Personal Data collected that is in direct relation to realizing the business functions of the Organization's products or services, meaning that such functions of its products or services would fail without collecting such Personal Data.

5.2.3 The amount of Personal Data obtained should be the minimum that is necessary for realizing the business functions of Organization's products or services.

5.2.4 When automatically collecting Personal Data, the Organization should make sure that the frequency of collection is the minimum necessary for realizing the business functions of its products or services.

5.3 Access Limitation

The Organization will establish a minimum access control policy for employees and other personnel, under which they have access and operating rights to Personal Data only to the minimum extent necessary to perform their duties.

5.4 Retention Limitation

5.4.1 Storage of Personal Data is limited to the shortest period of time necessary to realize the purposes of use consented by the Individual, unless otherwise specified by laws and regulations or agreed by the Individual.

5.4.2 Upon expiry of the agreed or permitted time limit for storage of the Personal Data, the Organization will delete or anonymize the Personal Data in a timely manner.

6. RIGHTS OF INDIVIDUALS

6.1 Introduction

The China Applicable Regulations provide various rights for Individuals whose Personal Data the Organization has possession or control. Such rights currently include access to, correction, deletion and de-registration of, and to request a copy of, his or her Personal Data. Details of these rights are provided below.

6.2 Access

6.2.1 Within 30 days upon receiving an access request, the Organization will provide the requesting Individual with access to the following information, relating to and/or provided by such Individuals:

(a) the Personal Data or the type of such Personal Data controlled by the Organization;

(b) the source of such Personal Data and the purposes for which such Personal Data is used; and

(c) the identities or types of third parties that have been provided such Personal Data.

6.3 Correction

Where an Individual finds that his or her Personal Data the Organization possesses is inaccurate or incomplete, the Individual has the right to request correction and the Organization should take necessary measures to correct or supplement such inaccurate or incomplete Personal Data within 30 days upon receipt of such request.

6.4 Requests for Copies Of Personal Data

Within 30 days upon receiving the request of any Individual, the Organization will allow such Individual to obtain or directly transfer a copy of the following types of his or her Personal Data to a third party designated by such Individual, to the extent practically feasible;

(a) Basic Personal Data, such as name, date of birth, gender, ethnic group, nationality, family relation, address, personal phone number, email address, etc.;

(b) Personal identity data, such as ID card, passport, driver's license, employee ID, social security card, resident certificate and any data therein;

(c) Personal health and physiological data, means the records generated during medical treatment, such as pathological information, hospitalization records, test reports, fertility information, family illness history, present illness history, infection history, etc.; and

(d) Personal education and occupation data, such as position, work unit, educational background, educational experience, training records, etc.

6.5 Deletion

6.5.1 The Organization must delete the Personal Data of an Individual pursuant to this Section 6.5 unless an exception under Section 6.7 applies.

6.5.2 The Organization must delete an Individual's Personal Data within 30 days upon the request of such Individual, and where the Organization collects or processes the Personal Data in a way that violates the provisions of laws and regulations, or its agreement with such Individual.

6.5.3 The Organization must delete an Individual's Personal Data where the agreed or permitted time limit for storage of the Personal Data has expired.

6.5.4 Further to the above:

(a) the Organization must cease sharing or transferring the Personal Data immediately, and instruct any third party, to which party the Organization has shared or transferred the Personal Data, to delete the Personal Data in a timely manner; and

(b) the Organization must immediately cease the public disclosure of the Personal Data, and issue a notice requiring related recipients to delete the Personal Data concerned where it has publicly disclosed the Personal Data.

6.6 De-registration

6.6.1 If the Organization provides products or services through registered accounts, the Organization should provide the Individuals with easily and conveniently available method(s) to de-register his or her account; and

6.6.2 Upon such Individual's de-registration of his or her account, the Organization should delete or anonymize his or her Personal Data in a timely manner. If it is necessary to retain such Personal Data pursuant to any law or regulation, such Personal Data should not be used in daily operations.

6.7 Exception

The Organization may reject any request of an Individual under Section 6.2 through Section 6.6 hereof, under certain circumstances, including but not limited to,

(a) where the request is in relation to Organization's performance of obligations specified in laws and regulations;

(b) where the request is in direct relation to State security or national defense security;

(c) where the request is in direct relation to public security, public sanitation, or major public benefits;

(d) where the request is in direct relation to investigations into crimes, prosecutions, court trials, execution of rulings, etc.;

(e) where the Organization has sufficient evidence to prove that the Individual is subjectively malicious or abuses his or her rights;

(f) where the request may influence significant legal rights and interests, such as the life and property, of the Individual or others, and it is difficult for the Organization to obtain the Individual's consent;

(g) where a response to such request will give rise to serious damage to the legal rights and interests of such Individual or to any other Individual or organization; and

(h) where the request involves any trade secrets.

If the Organization refuses the Individuals' request, the Organization must provide the Individual with a complaint channel as specified in Section 10.2.

7. PROTECTION AND SECURITY OF PERSONAL DATA

7.1 Introduction

The Organization may retain Personal Data for as long as such Personal Data is necessarily required or relevant for the purposes for which it was collected, and must maintain reasonable and appropriate safeguards and security measures to avoid Personal Data being leaked,

destroyed or lost, and protect the confidentiality, completeness and availability of Personal Data.

7.2 De-identification And Anonymization

7.2.1 To the extent practicable, the Organization should take steps to de-identify Personal Data after collection in a timely manner, and take technical and management measures to store the de-identified data separately from data that can be restored to identify Individuals. De-identification refers to a process whereby Personal Data is technologically processed to make it impossible to identify Individuals without the aid of additional data.

7.2.2 The Organization should delete or anonymize Personal Data in a timely manner upon expiry of the agreed or permitted time limit for storage of the Personal Data. Anonymization refers to an irreversible process whereby Personal Data is technologically processed to make Individuals unidentifiable, and the Personal Data cannot be restored to its previous state once processed.

7.3 Encryption

7.3.1 For the security of personal sensitive data, the Organization should employ encryption or other technological measures while transferring and storing such personal sensitive data.

7.3.2 Personal sensitive data refers to Personal Data that may cause harm to personal or property security, or is very likely to result in damage to an Individual's personal reputation or physical or mental health or give rise to discriminatory treatment, once it is leaked, unlawfully provided or abused. The types and examples of personal sensitive data can be described as follows.

(a) personal property data: bank account, bank deposit information, real estate information, credit record, etc.

(b) physiological and health data: the records generated during medical treatment, such as pathological information, hospitalization records, test reports, fertility information, family illness history, present illness history, infection history, etc.

(c) personal biometric data: fingerprint, palm print, facial recognition features, etc.; and

(d) personal identity data: ID card, passport, driver's license, employee ID, social security card, resident certificate, etc.

7.4 Records Of Personal Data Processing

The Organization should establish, maintain and update the records of activities conducted to process Personal Data, and the content of the records should at least include,

(a) Basic information, such as the type, amount and source of the Personal Data involved; and

(b) Processing information, such as purposes and scenarios of processing, system and personnel involved, etc.

7.5 Personal Data Security Impact Assessment

The Organization should establish a system for Personal Data security impact assessment, assess and deal with the security risks arising from the processing of Personal Data, formulate and retain assessment reports.

7.6 Data Breach Management Plan

K&S has developed an emergency response plan for potential Personal Data security incidents, in the event where the Personal Data that is possessed or controlled by the Organization is found to have been leaked, tampered with, or lost ("**Incidents**").

8. TRANSFER LIMITATION

8.1 Introduction

The Organization must not transfer Personal Data, including intercompany transfers, without ensuring that such process is in accordance with the China Applicable Regulations, and is advisable to take certain management measures before it conducts any Personal Data transfer activities.

8.2 Conclude Contracts

The Organization should specify, comprehensively and meticulously, the responsibilities and obligations of the data recipient through contracts with the data recipients. The specific provisions of the contract include the purpose, type, time limit for retention, responsibility of the recipient, and the rights of Individuals.

8.3 Self-security Assessment

The Organization should conduct a security impact assessment of Personal Data prior to transferring such data, and take effective measures to protect the Individuals based on the assessment results.

8.4 Transfer Records

The Organization should accurately record and store information about Personal Data transfers, including especially the type, scale, purpose of the sharing and transfer, and basic information of the data recipient.

8.5 Supervision of Data Recipients

Where the Organization discovers that a data recipient has processed the Personal Data in violation of the requirements of China Applicable Regulations or the contract terms, the Organization should immediately request the data recipient to cease relevant activities and to take effective remedial measures to control or eliminate the security risks affecting the Personal Data; if necessary, the Organization should terminate its business relationship with the data recipient, and request the data recipient to timely delete the Personal Data obtained from the Organization.

8.6 Assistance with Individuals' Rights

The Organization should assist Individuals to understand the processing activities of their Personal Data by data recipients, as well as the rights of the Individuals, such as the right to access, correct, delete their Personal Data and to de-register their accounts.

8.7 Cross-border Transfers

8.7.1 Where the Organization intends to provide Personal Data outside the territory of China due to business or other needs, the Organization should take the measures as specified in Section 8.2 to Section 8.6 above;

8.7.2 The self-security assessment for cross-border data transfer is recommended to be conducted primarily from four perspectives - purpose, security risk, performance and contract:

(a) Purpose - whether the transfer fulfills the requirements of legality, legitimacy, and necessity;

(b) Security risk - the risk posed by the transfer by taking into account the types, sensitivity, quantity, and scope of the Personal Data, and the conditions of the technical processing that the Personal Data undergoes;

(c) Performance - the past personal data protection and cyber security performance of both the Organization as the Personal Data transferor, and recipients; and

(d) Contract - whether the terms and conditions of the contract are sufficient to protect the legitimate rights and interests of the Individuals and whether the contract can be effectively performed.

9. NOTIFICATION

9.1 Introduction

Under the China Applicable Regulations, where an Incident occurs, the Organization should notify in a timely manner the affected Individuals and further report to the relevant competent authorities.

9.2 Incident Records

Where an Incident occurs, the Organization must immediately compile records of all details about the Incident, including but not limited to who detected the incident, when and where the Incident took place, the Personal Data concerned and the number of Individuals involved, the name of the compromised system, effects on other interconnected systems, and whether any law enforcement authority has been notified.

9.3 Notifications to Individuals

9.3.1 Where an Incident occurs that may seriously jeopardize the legal rights and interests of Individuals, for example, personal sensitive data has been leaked, the Organization should promptly notify each affected Individual of the particulars of the Incidents, by means of e-mails, letters, calls or push notifications. Where it is difficult to notify all affected Individuals one by one, the Organization may issue alerts in relation to the general public in reasonable and effective measures.

9.3.2 The content of notifications regarding Incidents should include at least the following:

(a) details of the Incident and its impact;

(b) what measures have been or will be taken to address the Incident;

(c) advice on what actions Individuals can take to protect themselves and reduce risk; and

(d) remedial measures available for Individuals.

9.4 Report to Competent Authorities

Generally, reporting to the competent authorities is required where an Incident occurs involving a leakage of Personal Data of at least 100,000 Individuals. If you discover or suspect an Incident has occurred, please report it immediately to the Data Protection Officer. The Data Protection Officer will determine whether it is mandatory for the Organization to report this Incident to the relevant competent authorities.

10. DATA PROTECTION OFFICER

10.1 Data Protection Officer

Employees or other personnel in China should consult with the Data Protection Officer if there are any queries regarding this China Policy or any data protection matters. Details pertaining to the Data Protection Officer can be found under K&S' Global Data Protection Policy.

10.2 Complaints

If any employee or other personnel has complaints regarding the Organization's data protection practices, please contact the Data Protection Officer. The Data Protection Officer will use good faith efforts to investigate each complaint and respond to a complaint within a reasonable time.