KULICKE & SOFFA ASIAPAC INC.
GLOBAL DATA PROTECTION POLICY – TAIWAN ADDENDUM/POLICY

GLOBAL DATA PROTECTION POLICY - TAIWAN ADDENDUM/POLICY
KULICKE & SOFFA ASIAPAC INC.

1. INTRODUCTION

1.1 Background To the Personal Data Protection Act

1.1.1 The Personal Data Protection Act (the "**PDPA**") is intended to be a baseline law for the protection of personal data in Taiwan and of Taiwan citizens generally.

1.1.2 The most recent version of the PDPA was enacted in 2015. It is enforced and administered by the Ministry of Justice, National Development Council and by industry-specific regulating agencies.

1.1.3 The PDPA is applicable to Kulicke & Soffa Asiapac Inc. (referred to as the "**Organization**") and the Organization is committed to complying with it.

1.2 Background to Taiwan Addendum/Policy

1.2.1 This Taiwan Addendum/Policy (the "**Taiwan 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 Taiwan Policy, all other terms and principles in the Global Data Protection Policy shall continue to apply. The Taiwan Policy shall apply to all K&S entities incorporated in Taiwan and all processing of personal data by K&S in Taiwan.

1.2.2 This Taiwan 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 Taiwan Addendum/Policy Part Of Employment Contract

1.3.1 All employees and agents of the Organization must strictly comply with this Taiwan Policy. For employees of the Organization, this Taiwan 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 Taiwan Policy from time to time. Any such amended Taiwan 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 Taiwan Policy seeks to provide each employee with a broad summary overview of the requirements of the PDPA and an understanding of the PDPA's impact on operational activities. For detailed information on the obligations and exceptions under the PDPA, you may refer to the PDPA itself as well as the relevant enforcement rules.

1.4 What To Do If You Are Aware Of Or Suspect A Breach of the PDPA

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

2. OVERVIEW OF THE PDPA

2.1 Key Definitions

2.1.1 The PDPA uses some key terms that are specifically defined therein, which are useful to know for the purpose of complying with its requirements and are also used in the Taiwan Policy. These definitions include:

(a) "**Personal Data**": information that may be used to directly or indirectly identify a natural person;

(b) "**Process,**" "**Processes**" or "**Processing**": the act of recording, inputting, storing, compiling/editing, correcting, duplicating, retrieving, deleting, outputting, connecting or internally transferring data for the purpose of establishing or using a Personal Data file;

(c) "**Use**" or "**Using**": the act of using Personal Data via any methods other than Processing;

(d) "**Data Subject**": an individual whose Personal Data is collected, Processed or Used.

(e) "**Sensitive Personal Data**": data pertaining to a natural person's medical records, healthcare, genetics, sex life, physical examination and criminal records.

(f) "**Commissioned Agency**": anyone to which Personal Data activities have been outsourced.

2.2 The Data Protection Principles Applicable To Personal Data

2.2.1 When dealing with Personal Data of any individuals, the Organization and all employees are required to adhere to the following key **data protection principles**:

(a) Lawful Basis;

(b) Purpose and Retention Limitation;

(c) Notification;

(d) Security Standards;

(e) Right of Access;

(f) Right of Correction, Cessation, and Deletion;

(g) Transfer Oversight; and

(h) Accountability,

(the above data protection principles may be referred to in the Taiwan Policy as the "**data protection principles**").

3. THE LAWFUL BASIS PRINCIPLE

3.1 Introduction

3.1.1 Under the PDPA, the Organization must have a lawful basis to collect, Process or Use Personal Data. The lawful bases are set forth in the PDPA.

3.2 The Lawful Bases Must be One of the Following:

3.2.1 For all Personal Data except Sensitive Personal Data, the following bases are permitted by the PDPA:

(a) where it is expressly required by law;

(b) where there is a contractual or quasi-contractual relationship between the non-government agency and the Data Subject, and proper security measures have been adopted to ensure the security of the Personal Data;

(c) where the Personal Data has been disclosed to the public by the Data Subject or has been made public lawfully;

(d) where it is necessary for statistics gathering or academic research by an academic institution in pursuit of public interests, provided that such data, as Processed by the data provider or as disclosed by the data collector, may not lead to the identification of a specific Data Subject;

(e) where consent has been given by the Data Subject;

(f) where it is necessary for furthering the public interest;

(g) where the Personal Data is obtained from publicly available sources unless the Data Subject has an overriding interest in prohibiting the Processing or Use of such Personal Data; or

(h) where the rights and interests of the Data Subject will not be infringed upon.

3.2.2 For Sensitive Personal Data, the bases are more restricted. Generally, private entities may only collect Sensitive Personal Data with the explicit consent of the Data Subject, given in writing. It may also be collected when the Data Subject has made the data publicly available, where necessary for academic research (if the data is anonymized), or upon the direction of a government agency in order to fulfill a legal obligation, so long as heightened security measures are adopted to protect the Sensitive Personal Data.

3.3 Forms of Consent

3.3.1 Consent is only one of the bases on which Personal Data may be collected. It is typically the only basis on which Sensitive Personal Data is collected, in which case the consent must be in writing. However, for ordinary Personal Data, consent can be given in any form, but it must come after the notification required by the PDPA, which is discussed as the "Notification Principle" below. Consent may be presumed if the Data Subject does not indicate an objection, and affirmatively provides his/her Personal Data after the Organization informs the Data Subject of the information required by the Notification Principle.

3.3.2 Consent to new purposes must be given separately after receiving notice of the new data uses. If the new purposes are founded on the basis of receiving consent, then the Organization must also include a statement about the impact on the Data Subject's rights and interests if the Data Subject does not consent to the new purposes or uses.

4. THE PURPOSE AND RETENTION LIMITATIONS PRINCIPLE

4.1 The Duty of Good Faith

4.1.1 Even after the Organization has established that its data collection and Use is done on a lawful basis, the PDPA requires any person or entity that collects, Processes, or Uses Personal Data (herein referred to as a "**Data Handler**"), to conduct their activities in a good faith manner. The obligation is connected to the purposes of collecting and Using Personal Data. Any Data Handler cannot Use Personal Data in a way that is outside the scope of the initial, specific

purpose for which the Personal Data was collected. All data Processing and Use must have legitimate and reasonable connections with the purposes of collection.

4.2 Limitations on New Purposes

4.2.1 If the Organization discovers a new purpose for Using Personal Data already in its possession, or acquires Personal Data for a purpose other than the one at the core of the data's original collection, it may face additional obligations towards the Data Subjects. These may include to obtain consent if the original basis for the collection did not rely on consent or have another lawful basis, or, when Using the Data Subject's Personal Data for a new marketing purpose, to provide the Data Subject of the ways (at the Organization's cost) that he/she can object to such Use. Any new purposes must be justified on one of a separate list of lawful bases, which are:

(a) where it is expressly required by law;

(b) where it is necessary for furthering public interests;

(c) where it is to prevent harm on life, body, freedom, or property of the Data Subject;

(d) where it is to prevent material harm on the rights and interests of others;

(e) where it is necessary for statistics gathering or academic research by a government agency or an academic institution for public interests; provided that such data, as provided by the data provider or disclosed by the data collector, may not lead to the identification of a specific Data Subject;

(f) where consent has been given by the Data Subject; or

(g) where it is to protect the Data Subject's rights and interests.

4.3 Retention Limitations

4.3.1 All Data Handlers must not retain data for longer than the existence of the purpose for its collection, or, as the case may be, for as long as a specific time period to which the Data Subject has agreed. As soon as the collection purpose or specified time period expires, the Organization must delete or cease Processing or Using the Personal Data.

4.3.2 There are exceptions to this obligation. The exceptions include where there is a statutory obligation to retain the data longer, and where the Data Subject agrees to a longer retention period in writing.

4.3.3 The enforcement rules under the PDPA clarify some examples of when the purposes of data collection no longer exist. These situations include, but are not limited to:

(a) where an organization dissolves, or ceases doing whatever business needs the Personal Data; and

(b) the goal envisioned behind the collection of the Personal Data has been accomplished or becomes impossible.

4.4 If a Violation is Discovered

4.4.1 Where Personal Data has been obtained as a result of a violation of the PDPA, that data must be deleted or not collected, Processed or Used any longer.

5. THE NOTIFICATION PRINCIPLE

5.1 Informing the Data Subject

5.1.1 Under PDPA Article 8, “when collecting” Personal Data from a Data Subject, the Organization and any outside agency commissioned by it to collect Personal Data must inform the Data Subject about certain information. These are:

(a) the name of the collector (i.e.: the Organization or an outside Commissioned Agency commissioned by the Organization to collect Personal Data);

(b) the purpose of the collection (which can include identifying subsequent collectors for whom the data is initially collected);

(c) the types of Personal Data to be collected;

(d) the time period, territory, recipients and methods by which the Personal Data is Used;

(e) the Data Subject's rights under the PDPA and methods for exercising such rights; and

(f) the Data Subject's rights and interests that will be affected if he/she elects not to provide his/her Personal Data.

5.2 Exceptions to the Notification Principle

5.2.1 The obligation to inform a Data Subject of the above does not apply in a narrow set of circumstances. These include:

(a) where collection is necessary for the Organization to perform a statutory obligation;

(b) where giving notice will prevent a government agency from performing its statutory duties;

(c) where giving notice will harm public interests;

(d) where the Data Subject already knows the same specific information to be included in the notification; or

(e) where the collection of Personal Data is for non-profit purposes and clearly has no adverse effect on the Data Subject.

5.3 What if the Organization Obtains Personal Data Secondhand?

5.3.1 When a Data Handler wishes to Process or Use data but it did not collect the data directly from the Data Subject concerned, PDPA Article 9 also requires that that Data Handler notify the Data Subject. This notice must include the same information as listed under 5.1 above (except 5.1.7), as well as from where it obtained the data.

5.3.2 This requirement does not apply to the following situations:

(a) any of the same exceptions listed under 5.2 above;

(b) where the Personal Data has been disclosed to the public by the Data Subject or has been made public lawfully;

(c) where the data Processor/User is unable to inform the Data Subject or his/her statutory representative;

(d) where the Use is necessary for statistics gathering or academic research in pursuit of public interests, provided that such data, as Processed by the data provider or as disclosed by the data collector, may not lead to the identification of a specific Data Subject; or

(e) where the Personal Data is collected by mass communication enterprises for the purpose of news reporting for the benefit of public interests.

6. THE SECURITY STANDARDS PRINCIPLE

6.1 Introduction

6.1.1 The PDPA imposes an obligation on all Data Handlers to keep Personal Data secure. This obligation may be supplemented by industry-specific data maintenance plans, which are published by the regulating agencies charged with oversight of a particular industry. As yet, there are no industry-specific maintenance plans promulgated by the regulating agency which oversees the Organization in Taiwan.

6.2 The Scope of the Security Obligation

6.2.1 There is no specific standard set in the PDPA for securing Personal Data. However, the PDPA does offer guidelines in its general Enforcement Rules. These guidelines offer a set of factors, which an organization may use to evaluate its own security practices and assess whether they are proper. The rigor with which data must be guarded depends on the nature and purposes of the personal-data activities involved. The existence of more factors in an organization's practices makes it more likely that they will be found to be adequate by a regulator.

6.2.2 The factors offered by the PDPA guidelines include:

(a) allocating management personnel and reasonable resources;

(b) defining the scope of Personal Data;

(c) establishing a mechanism of risk assessment and management of Personal Data;

(d) establishing a mechanism for preventing, giving notice of, and responding to a data breach;

(e) establishing an internal control procedure for the collection, Processing, and Use of Personal Data;

(f) managing data security and personnel;

(g) promoting awareness, education and training;

(h) managing physical facility security; and

(i) establishing an audit mechanism of data security.

7. THE RIGHT OF ACCESS

7.1 Introduction

7.1.1 Data Subjects are guaranteed a number of rights under Article 3 of the PDPA with respect to their Personal Data. These rights cannot be waived by contract. Among these rights are the right to request access to or a copy of one's own Personal Data records.

7.2 How to Respond to Requests

7.2.1 The PDPA requires Data Handlers to respond to requests for access or copies of Personal Data from the Data Subject within 15 days of receiving the request. The Organization may extend this period by another 15 days, but it must notify the Data Subject about the extension.

7.2.2 Generally, a Data Handler must provide access to or copies of the Data Subject's own Personal Data records to the Data Subject on the subject's request. However, a Data Handler can refuse to comply if national security or other national interests may be harmed by complying with the Data Subject's request, if complying with the Data Subject's request would prevent a government agency from executing its duties, or if any third party's life, health, freedom, properties, or other material interests may be harmed by complying with the Data Subject's request.

7.2.3 The PDPA permits a Data Handler to charge a reasonable fee to the Data Subject to cover the costs of provided access or copies of Personal Data.

8. THE RIGHTS OF CORRECTION, CESSATION AND DELETION

8.1 Introduction

8.1.1 A Data Subject has the right under the PDPA to request that inaccurate Personal Data be corrected, or to request that the Data Handler ceases to collect, Process, or Use their Personal Data, or to request that their Personal Data be deleted. These rights may never be waived or limited contractually.

8.2 When to Respond to Requests

8.2.1 The PDPA requires Data Handlers to respond to requests from the Data Subject for correction, cessation, or deletion of Personal Data within 30 days of receiving the request. The Organization may extend this period by another 30 days, but it must notify the Data Subject about the extension.

8.3 Requests for Correction

8.3.1 The PDPA imposes an obligation on a Data Handler to ensure the accuracy of Personal Data in its possession. Thus, if a Data Subject notifies the Organization that their Personal Data is incorrect, the Organization must correct the data record. However, the Organization may demand an explanation from the Data Subject about the need to correct the data (under PDPA Enforcement Rules Article 19). If the Organization disputes the correction offered by the Data Subject, then the Organization must delete or cease Using that Personal Data. The Organization may continue to retain the Personal Data if it is necessary to comply with a retention period prescribed by law or by contract, or if there are sufficient reasons to believe that the deletion of the Personal Data will infringe upon the Data Subject's interests that warrant protection, or if the Data Subject agrees to the further retention. However, the Organization must make a record of the dispute. If the Organization has failed to maintain accurate Personal Data, then it must alert any persons who have been provided with such Personal Data after it has been corrected.

8.4 Requests for Cessation or Deletion

8.4.1 For other purposes, the Organization must generally comply with such a request, unless further retention is necessary to comply with a retention period prescribed by law or by contract, or if there are sufficient reasons to believe that the deletion of the Personal Data will infringe upon the Data Subject's interests that warrant protection, where there are other legitimate reasons for not erasing it, or if the Data Subject has agreed to the further retention in writing.

9. THE TRANSFER OVERSIGHT PRINCIPLE

9.1 Introduction

9.1.1 The PDPA envisions oversight of data transfers in two contexts: cross-border transfers, and transfers resulting from outsourcing. Cross-border transfers may be subjected to oversight from the government, while for outsourcing activities it is left to the outsourcing entity to handle oversight.

9.2 Cross-border Transfers

9.2.1 There are no blanket restrictions on transferring Personal Data from within Taiwan to outside of Taiwan. However, the government has reserved the power to impose restrictions under certain circumstances. These circumstances include:

(a) where major national interests are involved;

(b) where an international treaty or agreement stipulates to that effect;

(c) where the country receiving the Personal Data lacks proper regulations on protection of Personal Data and the Data Subjects' rights and interests may consequently be harmed; or

(d) where the cross-border transfer of the Personal Data is carried out in order to circumvent the PDPA.

9.2.2 If any of these circumstances occur, the government will likely order the Organization to limit or cease the relevant cross-border transfers. Failure to comply with such an order may lead to serious penalties, especially in the event of intentional circumventions of the PDPA. Organization personnel tasked with managing Personal Data activities should remain alert to any orders or any public decisions by the Taiwan government concerning cross-border data transfers.

9.3 Outsourcing Activities

9.3.1 The PDPA requires that any outsourcing of data-Processing activities be accompanied by oversight. This oversight typically takes the form of provisions in the contract between the ultimate data User and the entity to whom Processing activities are outsourced.

9.3.2 If the Organization outsources any Personal-data Activities to other organizations, it may be held liable if it fails to supervise the actions of the Commissioned Agency. To ensure proper supervision is in place, the Organization must place these terms into contracts with the Commissioned Agency:

(a) the planned scope, category, specific purposes and time periods of the collection, Processing or Use of Personal Data;

(b) the measures taken by the Commissioned Agency in accordance with the Security Standards Principle;

(c) which third parties, if any, to be further commissioned by the Commissioned Agency;

(d) the information that must be notified to the Organization and the remedial measures that must be taken in the event that the Commissioned Agency or its employees violate(s) the PDPA or other laws or regulations relating to the protection of Personal Data;

(e) any reserved matters for which the Commissioned Agency is required to obtain prior instructions from the Organization; and

(f) the return of all media containing Personal Data and the deletion of any Personal Data stored and possessed by the Commissioned Agency due to its performance of the contract between the Organization and the Commissioned Agency, upon the termination or cancellation of the contract.

9.3.3 The Organization must also periodically inspect any Commissioned Agencies to ensure that the Commissioned Agency has complied with its obligations under the PDPA.

9.3.4 Commissioned Agencies are prohibited from Using Personal Data outside the directives incumbent to their engagement. They must also inform the Organization if they conclude that any activities of the outsourcing operation may violate the PDPA.

10. THE ACCOUNTABILITY PRINCIPLE

10.1 Introduction

10.1.1 Data Handlers are held liable under the PDPA for violating the responsibilities the law imposes on them or the rights it grants to Data Subjects. It is important that the Organization maintain good relationships with the Data Subjects whose data it Processes, and make every effort to respect the individual rights of Data Subjects.

10.1.2 Government agencies may also spontaneously audit and inspect the physical facilities and procedures of any company that handles Personal Data. The Organization must remain diligent in its compliance with the terms of the PDPA to demonstrate to any potential inspection that it takes data protection seriously.

10.2 Handling security incidents

10.2.1 Part of the responsibility is to keep Data Subjects informed of any significant developments that affect their Personal Data. If any Personal Data is stolen, disclosed, altered, or otherwise infringed upon, the Data Subject must be notified after the facts have been clarified. No specific timeline for providing this notice is provided by law, other than “after the relevant facts have been clarified” (PDPA Article 12).

10.2.2 A notification to Data Subjects about a security incident may take the form of verbal words or in writing, so long as such means can communicate the information known or available effectively to the affected Data Subjects.

10.2.3 The Organization may also notify the Data Subjects through the Internet, the media, or other appropriate public means.

10.2.4 The content of these notifications must include the facts pertaining to the data breach and the response measures the Organization will be adopting or has already adopted to address the breach.

10.2.5 There is no general requirement provided by the PDPA to notify any regulatory authority of breach events.