

KULICKE AND SOFFA INDUSTRIES, INC.

GLOBAL DATA PROTECTION POLICY

1. Introduction

Kulicke and Sofa Industries, Inc. and its subsidiaries (collectively and individually, "**K&S**") hereby demonstrate our commitment to privacy and the protection of Personal Data (as defined below), by establishing a global data protection program to support compliance with applicable privacy and/or Personal Data protection laws and standards for protecting Personal Data. This Global Data Protection Policy (the "**Policy**") provides a general framework and sets out the requirements for ensuring that K&S Process (as defined below) Personal Data in a fair, lawful, transparent and secure way, whether locally or globally.

The obligation to safeguard Personal Data rests with every K&S employee and temporary staff, officer and director (collectively, "**Employees**") and Relevant Party (as defined below) who has access to Personal Data. Each department is responsible for ensuring that privacy and Personal Data protection law requirements are assessed at an early stage and appropriate privacy and Personal Data protection controls are in place within their department. Employees are encouraged to consult with their functional heads whenever in doubt about the best course of action in a particular situation.

Because this Policy cannot address every issue that may arise, we expect that Employees will use their common sense, act prudently, professionally, with clarity of intention and in compliance with applicable privacy and/or Personal Data protection laws. Always consider what a reasonable person would consider appropriate in the circumstances. When in any doubt, you are to reach out to your Data Protection Officer for guidance.

This Policy seeks to provide a general framework for K&S to comply with the principles of applicable privacy and Personal Data protection laws and regulations. It sets out the global minimum standards to which all of K&S' Employees and Relevant Parties must comply when Processing or handling Personal Data in the course of carrying out work for or on behalf of K&S. In some cases, local laws and regulations may be more restrictive or strict than this Policy; where that is the case, the more restrictive or strict rules, laws and regulations must be followed when Processing and/or handling Personal Data in that jurisdiction. Accordingly, local addenda, where applicable, would/may be issued and/or updated from time to time. The relevant K&S entity and Individuals are expected to adhere to both the Policy as set out herein and the local addendum, if any, that is applicable to their jurisdiction, and shall not be subject to the local addenda of other jurisdictions. In the event of inconsistency between the local addendum for a particular jurisdiction and this Policy, the local addendum shall prevail to the extent of inconsistency.

Whilst this Policy stipulates the minimum global standards for protecting Personal Data, K&S will only do so to the extent required by law or regulation and, accordingly, this Policy will not provide additional rights, remedies or access rights to an Individual if such rights or remedies do not exist or are more restrictive in the jurisdiction where the Individual is located.

2. Compliance with this Policy

You must ensure that you read, understand and comply with this Policy.

A breach by K&S of its data protection responsibilities could result in a significant financial sanctions, negative publicity and damage to customer confidence. The protection of Personal Data in accordance with this Policy is the responsibility of all Employees.

This Policy applies to all Employees. A breach by an Employee of this Policy may result in appropriate disciplinary sanctions, including termination of employment or contract, for that Employee.

3. Definitions

"Data Intermediaries or Data Processors" means third party service providers which Process Personal Data on K&S' behalf. Examples of Data Intermediaries or Data Processors include payroll agencies, benefit administrator providers, data storage, hosting or warehousing providers, network, information technology, security or other service providers, market research and analytics firms and marketing companies. Whether a third party service provider to K&S is deemed a Data Intermediary or Data Processor under this Policy depends on the circumstances of its engagement with K&S. Please contact your Data Protection Officer if there are questions.

"Data Protection Officer" means the Individual who has been appointed as the data protection officer of a K&S entity.

"Individual" means a natural person, whether living or (where appropriate) deceased. Examples of Individuals are K&S': (i) employees, their family members and other individuals about whom K&S has Personal Data as a result of the relationships those individuals have with such employees; (ii) agency temporary staff; (iii) interns; (iv) potential candidates seeking employment with K&S; (v) shareholders; (vi) contractors; (vii) the staff of K&S' suppliers/customers; (viii) visitors to K&S' buildings or facilities; or (ix) users who visit any K&S website or otherwise any other K&S digital platforms. This Policy shall apply to the Personal Data of a deceased Individual at least to the extent required by applicable laws.

"PD Recipient" means a third party service provider (other than a Data Intermediary or Data Processor) or a third party organization, whose staff in the ordinary course of performance of services may access Personal Data in K&S' possession and control, or to which K&S may otherwise disclose to such staff Personal Data.

"Personal Data" means any data about an Individual who can be identified: (i) from that data; or (ii) from that data and other information to which K&S has or is likely to have access. Please refer to the respective local policies for special treatment in respect of particular types of Personal Data. In some jurisdictions, the local privacy or Personal Data protection law may specify additional requirements relating to sensitive Personal Data (see Section 5 of this Policy for details relating to processing sensitive Personal Data).

"Processing" means the carrying out of any operation on Personal Data, including, without limitation, collecting, using, disclosing, recording, holding, storing, copying, organizing, adapting, altering, retrieving, consulting, using, combining, transmitting, transferring, disclosing, disseminating, making available, correcting, erasing or destroying. For the purposes of this Policy, Processing includes any operation taken by K&S, its Data Intermediaries or Data Processors.

"Relevant Party" means, collectively, Data Intermediaries or Data Processors and PD Recipients.

4. Overarching principles

Without limitation to the other provisions set forth in this Policy, all Employees and all K&S departments must comply with the following overarching principles when processing or handling Personal Data:

- a. **Fairness and Transparency** K&S and its Relevant Parties will Process Personal Data fairly and provide Individuals with information about what, how and why their Personal Data is processed.
- b. **Lawful Processing** K&S and its Relevant Parties will only Process Personal Data lawfully where it has a valid basis for the processing.
- c. **Purpose Limitation** K&S and its Relevant Parties will only collect Personal Data for specific, explicit and legitimate purpose. Any subsequent Processing should be compatible with that purpose, unless K&S has obtained the Individual's consent or the Processing is otherwise permitted by law.
- d. **Data Minimization** K&S and its Relevant Parties will only Process Personal Data that is adequate, relevant and limited to the purpose for which it was collected.

- e. **Data Accuracy** K&S and its Relevant Parties will take reasonable steps to ensure Personal Data is accurate, complete and kept up-to-date.
- f. **Individual Rights** K&S and its Relevant Parties must allow Individuals to exercise their rights in relation to their Personal Data, including (where applicable) their rights of access, erasure, rectification, portability and objection, where such rights are provided for by applicable local privacy or Personal Data protection law.
- g. **Storage or Retention Limitation** K&S and its Relevant Parties will only retain Personal Data for as long as it is needed for the purpose for which it was collected, and in each instance not exceeding the duration permitted by applicable local privacy or Personal Data protection law.
- h. **Data Security** K&S and its Relevant Parties will use appropriate security measures to protect Personal Data.
- i. **Accountability** K&S and its Relevant Parties will take steps to comply with these principles and with applicable local privacy or Personal Data protection law.

Some of the above principles are elaborated further in the subsequent paragraphs of this Policy.

5. Processing Sensitive Personal Data

Depending on jurisdiction, certain Personal Data may be classified as “sensitive” or “special” and, accordingly, are subject to additional compliance requirements because they carry higher risks for an Individual if misused or Processed incorrectly. In some jurisdictions, misuse of sensitive Personal Data may incur higher penalties, monetary fines or even imprisonment.

The definition of sensitive Personal Data varies by jurisdiction, but can include:

Ethnic or racial origin, political opinions, religious or other similar (philosophical) beliefs, trade union and similar memberships, physical/mental health or disability details (including pregnancy or maternity information), gender identity or expression, sexual orientation, biometrics and genetics data, criminal or civil offenses, financial data and/or national identification numbers.

Employees must always treat any collection, use or storage of sensitive Personal Data with more scrutiny than Personal Data as they require additional or specific privacy, legal and security safeguards. In some jurisdictions, K&S may not process sensitive Personal Data unless first undertaking either a mandatory data protection impact assessment or privacy review.

6. Data Collection and Minimization

Personal Data must only be collected by fair and lawful means and in a transparent manner. Only the minimum amount of Personal Data required to support the purpose for which it was collected should be Processed.

Personal Data must not be made available to anyone, including Employees from other departments, who are not authorized to have the information or have no reason to access such Personal Data.

The means by which K&S may collect Personal Data may include, without limitation, the following ways:

- a. directly, via the completion of forms or submission of information to K&S in any way;
- b. from any K&S entity;
- c. automatically, when an Individual visit our websites or otherwise any other K&S digital platforms, using technologies such as cookies (either by K&S or a third party, in each instance subject to the applicable cookie policy);

- d. from other sources, such as prior employers, recruitment or temporary staffing agencies, credit agencies, law enforcement agencies and/or other public agencies;
- e. from any publicly available sources or records;
- f. via CCTV recordings when an Individual visits K&S' buildings or facilities; and/or
- g. by such other lawful means.

7. Getting Consent for Data Processing

As a global company, important business activities can only be carried out effectively and important business efficiencies can only be achieved by Processing and/or consolidating information about Individuals in specific and/or centralized databases and systems located at specific worldwide facilities. Such Personal Data is also or may also be shared with other systems and databases hosted by or on behalf of K&S. However, K&S and those other systems and databases will only Process such Personal Data in accordance with applicable laws, this Policy and any applicable local addenda, in connection with employment-related purposes or to support business purposes, which may include, without limitation, the list of purposes as set out in **Appendix A**. Examples of the types of Personal Data that K&S may Process may include, without limitation, the list set out in **Appendix B**. Examples of the classes of persons to whom Personal Data may be disclosed include, without limitation, the list set out in **Appendix C**.

Unless permitted by applicable privacy or Personal Data protection law, K&S shall not Process Personal Data for any purpose without the consent of the Individual. Consent may be oral or written, but Employees are encouraged to be prudent and to obtain consent in writing or some other recorded form whenever possible. In getting consent from an Individual, K&S shall provide the Individual appropriate information of all the purposes for which Personal Data is to be Processed. Individuals should note that some of the activities above may occur on a periodic basis, thereby warranting the periodic Processing of Personal Data; in such situations, it is sufficient that K&S obtains consent prior to the first collection or use of the Personal Data (save as provided under applicable local addenda).

K&S must consider the privacy or Personal Data protection risks before Processing Personal Data, such as using a new system or as part of a project. Where K&S wishes to use Personal Data for a new purpose that has not been notified to the Individual, unless exempted under applicable privacy or Personal Data protection law, K&S shall notify the Individual of the new purpose and gain his/her consent prior to such use of that Individual's Personal Data.

To the fullest extent permitted under applicable privacy or Personal Data protection law, every Individual who deals with K&S is required to consent to the Processing of Personal Data for the reasons and purposes, set out above or as the circumstance of Processing requires, and to the extent necessary depending on the relationship between K&S and such Individual.

8. Retention and Security of Personal Data

K&S may only retain Personal Data for as long as such Personal Data is necessarily required or relevant for the purpose for which it was collected, in each instance not exceeding the duration permitted by applicable privacy or Personal Data protection law. K&S shall not retain Personal Data longer than is necessary and shall securely return, dispose or destroy such Personal Data in a permanent and complete manner when it is no longer required.

Every K&S entity which Processes Personal Data shall maintain reasonable and appropriate safeguards and security measures to protect Personal Data in accordance with its sensitivity, from: (a) loss or theft, (b) unauthorized access, use or disclosure, (c) improper copying, modification or tampering, (d) improper retention or destruction, and (e) loss of integrity (each, a "**Loss**"). In the event of information security breaches or data breaches, K&S shall respond promptly and effectively.

There may be mandatory data breach notification requirements in a jurisdiction. Each Employee is to refer to his/her local addendum or any applicable data breach management plan to ensure that such mandatory requirements relating to data breach notification are complied with.

Every Employee that has access to, and/or Processes, Personal Data shall:

- a. periodically assess whether appropriate privacy controls and safeguards are in place within their department;
- b. take appropriate steps to prevent the above instances of misuse, loss, improper or unauthorized activities, work with relevant K&S stakeholders including the information technology department where necessary, and report any instance of Loss to the Data Protection Officer(s) (as listed in Section 15 below entitled "**Data Protection Committee**"); and
- c. review on a regular basis to determine if retention of Personal Data is still required.

9. Accuracy

An Employee must recognize that he/she is the main and critical source of Personal Data that is disclosed by him, or by a third party upon his instructions, to K&S. As such, each Employee disclosing Personal Data as contemplated herein (the "**Disclosing Employee**") shall:

- a. warrant and represent to K&S that the Personal Data disclosed (or instructed by the Disclosing Employee to a third party to disclose) to K&S, is authentic, accurate and complete;
- b. warrant and represent to K&S that the Personal Data of another natural person which the Disclosing Employee discloses (or instructs a third party to disclose) to K&S is authentic, accurate and complete, and that Disclosing Employee is authorized by such other person to make such disclosure; and
- c. shall inform the relevant K&S entity when there are any changes to the Personal Data which was previously disclosed by the Disclosing Employee to K&S, so as to ensure that K&S has the most current, accurate and complete information. Disclosing Employees should note that they should upload/update their Personal Data in the manner as advised by their Human Resources department.

K&S shall use reasonable efforts to ensure that the Personal Data it uses is sufficiently accurate and complete to minimize the possibility that incorrect Personal Data may be used to make a decision that impacts the Individual to whom the Personal Data relates, or if such Personal Data is likely to be disclosed to a third party. When a Disclosing Employee is relying on a third party to provide his/ her Personal Data to K&S, such Disclosing Employee shall, unless impracticable to do so, conduct independent verification or obtain confirmation from the third party that it has adequately verified accuracy and completeness of his/ her Personal Data provided to K&S.

10. Access and Correction of Personal Data and Rights of Individuals

Applicable privacy or Personal Data protection law may provide various rights to an Individual, vis-à-vis the Personal Data of the Individual that K&S has possession or control of. Such rights typically include access and correction rights. Refer to your local addenda for other rights that may be provided under the laws of your jurisdiction.

Upon an Individual's written request, K&S shall, within a reasonable timeframe or where applicable, within the statutory timeline, provide the Individual with information about the Personal Data relating to and/or provided by, the Individual, in K&S' possession or control. Depending on applicable local privacy or personal data protection law, K&S may have the right to charge the Individual reasonable fees and costs incurred by K&S to deal with such access right. K&S may refuse a data access request in certain situations. Please refer to the respective local addenda for details, if any.

Upon written request, K&S will, as soon as reasonably practicable or where applicable, within the statutory timeline, correct or complete any Personal Data relating to, or provided by, an Individual, in K&S' possession or control, which is inaccurate or incomplete. K&S may choose not to undertake correction or completion in certain situations. Please refer to the respective local addenda for details, if any.

11. Third Parties

When dealing with third parties, K&S remains responsible to protect Personal Data that is within K&S' possession or control. Hence, before disclosing Personal Data to any third parties, the Employee intending to carry out such disclosure and K&S, would need to ensure that applicable privacy or Personal Data protection law requirements regulating such disclosure has been complied with.

This could include, but not be limited to, obtaining consent from the Individual whose Personal Data is to be disclosed, implementing specific security measures, imposing contractual clauses on the third party who is a recipient of such Personal Data to adequately protect the disclosed Personal Data and ensuring that the disclosure is securely carried out.

Data Intermediaries or Data Processors

Data Intermediaries or Data Processors are expected to embrace standards of conduct consistent with the principles of this Policy and any applicable local addenda. K&S personnel who intend to contract with any Data Intermediary or Data Processor shall prior to engaging any Data Intermediary or Data Processor:

- a. assess the privacy risk of the Data Intermediary or Data Processor which includes but not be limited to an assessment of its state of compliance with local privacy or Personal Data protection law and an assessment of the security measures the Data Intermediary or Data Processor deploys to protect the Personal Data that it will be processing on behalf of K&S;
- b. provide such Data Intermediary with a copy of this Policy and any applicable local addenda and require it to sign an Acknowledgement substantially in the form set out in **Appendix D**;
- c. enter into a written contract with robust data protection clauses that are designed to ringfence the risks to K&S and to impose on the Data Intermediary or Data Processor strict requirements to protect the Personal Data it will be processing for K&S; and
- d. ensure that the Data Intermediary or Data Processor is given up-to-date instructions on the Processing of Personal Data (e.g. K&S shall notify relevant Data Intermediaries or Data Processor to cease Processing and to destroy Personal Data upon the termination of employment of any employee).

The Employee that is responsible for the engagement of the Data Intermediary or Data Processor shall ensure that throughout the lifetime of the contract, K&S continues to have continual oversight of the Data Intermediary's or Data Processor's processing of Personal Data on K&S' behalf, which shall include regular audit or assessments on whether the Data Intermediary is complying with its obligations to protect the Personal Data to the level expected by applicable privacy or Personal Data protection law.

PD Recipient

PD Recipients are expected to embrace standards of conduct consistent with the principles of this Policy and any applicable local addenda. K&S personnel who intend to contract with or disclose Personal Data to any PD Recipient shall prior to doing so:

- a. assess the privacy risk of the PD Recipient;
- b. provide such PD Recipient with a copy of this Policy and any applicable local addenda and require it to sign an Acknowledgement substantially in the form set out in **Appendix E**; and
- c. unless impracticable to do so despite attempts, impose appropriate contractual clauses on such PD Recipient to protect the Personal Data that the PD Recipient may be receiving from K&S or that it may be accessing.

12. International Transfers

K&S will not carry out international transfers of Personal Data (including intercompany transfers) without ensuring that the transfer is in accordance with the laws of the transferor's jurisdiction and that there is in the transferee's jurisdiction an adequate level of protection having regard to the level of protection afforded for those Personal Data under the transferor's policy and jurisdiction. The transferor is responsible to assess such adequacy and may request the recipient to adopt protections similar to those under the transferor's policy and jurisdiction.

13. Personal Data Inventory and Processing Documentation

Where required by applicable privacy or Personal Data protection law, K&S and the department that is/are intending to Process Personal Data, would be required to document K&S' Processing of Personal Data and its compliance with such applicable law, i.e. accountability.

This would include a description and compliance assessment of all K&S activities where Personal Data is processed by K&S or an Employee for K&S, which can include but is not limited to any Processing performed on Personal Data as part of an IT application, business process, outsourcing, third party cooperation or disclosure for specified purposes, etc.

14. Privacy by Design

K&S Employees must consider privacy or Personal Data protection as an integral component of the design, development, operation and management of every existing or new project, tool, application, internal service and offering which process Personal Data. When Employees engage vendors and partner organizations as part of any design, development and implementation work, privacy by design must also be an integral component.

15. Data Protection Committee

To oversee data protection matters, K&S has set up a Data Protection Committee sitting at its headquarters at 23A, Serangoon North Avenue 5, #01-01, K&S Corporate Headquarters, Singapore 554369 comprising representatives from the functions of Legal, Human Resources, Finance, Facilities, IT and Marketing Communications. Employees are encouraged to consult with their local and Singapore functional representatives if there are queries regarding this Policy. Alternatively, an Employee may contact any of the following Data Protection Officers.

Data Protection Officers:

Lim Zi Yao, Senior Manager, Legal Affairs: +65 6417 3265, zylim@kns.com

Johnson Ong, Senior Manager, HRMIS: +65 6880 9488, yeongsong@kns.com

Data Protection Committee Members:

Chua Boon Hwang, Global Payroll Manager: +65 6880 9603, bhchua@kns.com

Daniel Cheong, Manager, Facilities: +65 6880 9487, cscheong@kns.com

Marilyn Sim, Director, Marketing Communications: +65 6880 9309, msim@kns.com

Karen Yong, Senior Manager, Governance and Information Security: +65 6417 3428, ssyong@kns.com

If an Employee has any complaints, please contact any of the Data Protection Officers, who may direct the queries to the relevant functional representative of the Data Protection Committee. K&S will use good faith efforts to investigate each complaint and to respond within reasonable timeframes. K&S will deal with each complaint in a speedy, fair, impartial and unbiased manner.

No Employee will be victimized or prejudiced directly or indirectly as a result of lodging a complaint. K&S will endeavor to resolve each complaint within ten (10) working days, but when this is not

reasonably practicable (such as when an investigation requires a longer amount of time), the Employee will be advised accordingly.

Guidelines on escalation of a complaint:

- a. the aggrieved Employee shall provide adequate details of the complaint to the Data Protection Officers;
- b. written or verbal statements, where appropriate, would be obtained from the aggrieved Employee and other parties involved. Such statements shall be documented by the investigators; and
- c. Data Protection Officers will perform an investigation and respond to the aggrieved Individual.

An Employee shall not lodge malicious complaints or abuse the procedure by repeatedly lodging a complaint on the same matter. An Employee found to be in abuse of this Policy will be subject to disciplinary action.

16. General

Any waivers of this Policy and local addenda must be approved by any of the Data Protection Officers.

Subject to applicable law, K&S may revise and/or amend and/or supplement this Policy and local addenda at its discretion at any time or from time to time. Such changes will be published on K&S' intranet. Employees are advised to check K&S' intranet periodically to ensure that they are aware of any change, and to the fullest extent permissible under applicable laws, an Employee who deals with K&S agrees to be bound by the latest online version of this Policy and applicable local addenda.

APPENDIX A

NON-EXHAUSTIVE EXAMPLES OF PURPOSES

1. Recruitment (including retaining Personal Data of former employees), termination and succession planning
2. Workforce management and organization development
3. Payroll, benefit administration and management, compensation
4. Training and development and sponsored tuition
5. Reference checks and background checks
6. Performance, conduct and behavior evaluation and management
7. Problem resolution (grievances), internal investigations
8. Work related injury and any illness reporting
9. Any activity in connection with the managing or terminating of an employee relationship
10. Employee communications, newsletters, corporate displays and publications, corporate videos and photographs, participation in any K&S event (whether of a professional, social, recreational or other nature)
11. Administration of activities (e.g. Programs, conferences, workshops, exhibitions, contests, lucky draws, employee surveys) offered to, and participated by, Individuals
12. Auditing, compliance, risk management, emergency management
13. Budget, expense and other financial planning and management
14. Corporate, statutory or governmental registration, reporting, filing, declaration or other requirements
15. Legal proceedings, Governmental, regulatory or other investigations
16. Tracking, monitoring and surveillance purposes (including those related to hygiene, public health and safety, and security) unless prohibited by applicable privacy or personal data protection law
17. Authorizing, granting, administering, monitoring and terminating access to, or use of, K&S or third party systems, facilities and infrastructure
18. Due diligence
19. Any divestment of business
20. Any activity as required or authorized under applicable corporate policies, including but not limited to the Information classification and Security Policy and Information Security Policy
21. Any activity as required or authorized under applicable laws or regulations
22. Any other purpose necessary, ancillary or consequential to the above specified purposes

APPENDIX B

NON-EXHAUSTIVE EXAMPLES OF PERSONAL DATA

1. Contact information (e.g. Name, home or other mailing addresses, mobile or home contact numbers, fax numbers, personal email addresses, emergency contact information)
2. Personal information (e.g. Date of birth, personal identification number(s) or other social/national identification number(s), fingerprints, marital status, country of birth, nationality, citizenship, permanent residence status, race (ethnic origin), gender, religion, preferred language, bank account information, health condition(s) or other medical records, driver's license number, vehicle license plate number)
3. Photographs and other visual images or recordings
4. Employment, performance, compensation and benefits (e.g. Employment history and letters of recommendation, hire date, position/grade, attendance, goals/objectives, performance reviews, performance and leadership ratings, salary, allowances, bonus, incentives, equity or other awards, family member/ dependents' names and their relationship and dates of birth etc., grievance resolutions)
5. Work permits or restrictions
6. Agreements executed with K&S
7. Education and training (e.g. Education level and qualifications, field and institution, competency assessments, professional licenses, certifications and awards, training courses, records and test results)
8. Computer or facilities access and authentication information (e.g. Identification codes, passwords, employee identification numbers)

APPENDIX C

NON-EXHAUSTIVE EXAMPLES OF CLASSES OF PERSONS TO WHOM PERSONAL DATA MAY BE DISCLOSED

1. Parties to whom disclosure of information is necessary or desirable to enable K&S to fulfill employment-related purposes or to support business purposes
2. Parties to whom K&S is compelled or required to disclose information by law or in response to a Court order or a governmental or regulatory agency
3. Any party where public interest or K&S' interests require disclosure
4. A Data Intermediary
5. A PD Recipient
6. A party seeking employment references
7. A pension or insurance company with whom K&S has arranged benefits coverage for its employees
8. Related companies, subsidiaries, holding companies and associated companies in, and of, the K&S group of companies for internal management and marketing purposes
9. Parties to whom disclosure is made for one or more of the purposes set out in **Appendix A** or consented to by the Individual in question
10. Any other parties pursuant to consent provided by the Individual in question or where permitted by applicable privacy or personal data protection law

APPENDIX D

ACKNOWLEDGEMENT BY DATA INTERMEDIARY

We, [insert full name of Data Intermediary], with a principal place of business at [insert address of Data Intermediary], acknowledge and agree that we:

- a. have received and read a copy of the Kulicke and Soffa Industries, Inc. Global Data Protection Policy, including the applicable local addendum, (collectively, the "**Policy**");
- b. have policies and procedures in place consistent with, or at least equivalent to, the principles and standards of conduct of the Policy;
- c. shall comply with applicable privacy and data protection laws and regulations;
- d. will strictly follow your instructions on the Processing (as defined in the Policy) (including making required changes) of any personal data furnished by you (or upon your instructions) and only process personal data to the extent necessary to provide the scope of services as agreed between us;
- e. will not retain such personal data for longer than is necessary and shall securely return, dispose or destroy them in a permanent and complete manner when it is no longer required;
- f. will protect such personal data from: (i) loss or theft, (ii) unauthorized access, use or disclosure, (iii) improper copying, modification or tampering, (iv) improper retention or destruction, and (v) loss of integrity, and we will notify you immediately in the event of any information security breaches and cooperate with you in terms of any assistance, information requests, or investigations;
- g. will not transfer any personal data to any entity or person, or subcontract our obligations under our service agreement and hereunder, without getting your prior written consent; and
- h. will allow you to audit us to ensure our compliance with this Acknowledgement.

We shall indemnify you, your officers, directors, employees, controlling persons and customers against any loss, damage, expense, liability, proceedings, judgments or costs (including without limitation legal fees) arising out of or in connection with any unauthorized Processing, access or leakage of personal data (howsoever arising) or our breach of this Acknowledgement. In addition, we agree that you have the right to immediately terminate any services or service agreement(s) if there is any unauthorized Processing, access or leakage of personal data (howsoever arising) or if we breach this Acknowledgement.

Name:
Designation:
For and on behalf of [insert full name of Data Intermediary]
Date:

APPENDIX E

ACKNOWLEDGEMENT BY PD RECIPIENT

We, [insert full name of PD Recipient], with a principal place of business at [insert address of PD Recipient], acknowledge and agree that we:

- a. have received and read a copy of the Kulicke and Soffa Industries, Inc. Global Data Protection Policy, including the applicable local addendum, (collectively, the "**Policy**");
- b. have policies and procedures in place consistent with, or at least equivalent to, the principles and standards of conduct of the Policy;
- c. shall comply with applicable privacy and data protection laws and regulations;
- d. will inform our staff (whether or not they are required to be physically present at your premises) of the same and ensure that they adhere to (a) and (c) above;
- e. will strictly follow your instructions on the Processing (as defined in the Policy) (including making required changes) of any personal data furnished by you (or upon your instructions) and only process personal data to the extent necessary to provide the scope of services as agreed between us;
- f. will not retain such personal data for longer than is necessary and shall securely return, dispose or destroy them in a permanent and complete manner when it is no longer required;
- g. will protect such data from: (i) loss or theft, (ii) unauthorized access, use or disclosure, (iii) improper copying, modification or tampering, (iv) improper retention or destruction, and (v) loss of integrity, and we will notify you immediately in the event of any information security breaches and cooperate with you in terms of any assistance, information requests, or investigations;
- h. will not transfer any personal data to any entity or person, or subcontract our obligations under our service agreement and hereunder, without getting your prior written consent; and
- i. will allow you to audit us to ensure our compliance with this Acknowledgement.

We shall indemnify you, your officers, directors, employees, controlling persons and customers against any loss, damage, expense, liability, proceedings, judgments or costs (including without limitation legal fees) arising out of or in connection with any unauthorized Processing, access or leakage of personal data (howsoever arising) or our breach of this Acknowledgement. In addition, we agree that you have the right to immediately terminate any services or service agreement(s) if there is any unauthorized Processing, access or leakage of personal data (howsoever arising) or if we breach this Acknowledgement.

Name:
Designation:
For and on behalf of [insert full name of PD Recipient]
Date: