Kulicke & Soffa

KULICKE AND SOFFA INDUSTRIES, INC.

TOGETHER WITH ITS AFFILIATES INCORPORATED IN THE UNITED STATES

GLOBAL DATA PROTECTION POLICY – UNITED STATES ADDENDUM/POLICY

Kulicke & Soffa

GLOBAL DATA PROTECTION POLICY – UNITED STATES ADDENDUM/POLICY

KULICKE AND SOFFA INDUSTRIES, INC.

TOGETHER WITH ITS AFFILIATES INCORPORATED IN THE UNITED STATES

1. INTRODUCTION

1.1 Background To U.S. Data Privacy and Security Law

1.1.1 **Data Privacy Law**. There is no single, omnibus United States federal law addressing data privacy rights and obligations. Federal laws, which apply to residents in all states, are generally sector-specific and primarily regulate the financial and healthcare sectors, the telecom industry, government contractors and children. State laws, where they exist, more frequently look to protect consumers residing in that state, which is permitted under the United States system that allows states to regulate absent federal pre-emption or an undue burden on interstate commerce.

1.1.2 **Data Cybersecurity Law**. The United States does not have a single, comprehensive federal law regulating cybersecurity. Federal laws, which apply to residents in all states, are generally sector-specific and primarily regulate the financial and healthcare sectors, the telecom industry, government contractors and children. Industry groups have also undertaken self-regulatory efforts that are not law but are considered guiding principles and best practices. For example, the Payment Card Industry Data Security Standard (PCI-DSS) – a standard enforced by contract, not a law – provides security requirements for all entities accepting or processing payment transactions.

(a) Many states also have laws that protect the personally identifiable information of residents, but the level of protection and the types of information considered to be personally identifiable differ from state to state. Some states are more protective of data than others.

(b) All states in the United States, as well as the District of Columbia, Guam, Puerto Rico and the U.S. Virgin Islands, have enacted laws requiring notification in the event of a "security breach," "breach of security" or "breach of security of the system" (collectively referred to here as a "**security breach**"). Whether affected individuals, the states attorneys general and other agencies must or should be notified varies by jurisdiction and is a fact-specific determination. In the event of a suspected or actual security breach, refer to Section 3.9.

(c) In addition, at least 24 states have laws that address data security practices of private sector entities. Most of these state laws relate to entities that maintain personal information about residents of that state and require the entity to maintain "reasonable security procedures and practices" appropriate to the type of information and the risk.

1.1.3 **Applicability to the Organisation**. Among the states, the state with the most applicable privacy law to Kulicke and Soffa Industries, Inc. and its affiliates incorporated in the United States (a list is set forth as **Appendix B** to this policy) (collectively referred to as the "**Organisation**") is California. Currently, there are broad, privacy legal obligations on businesses that took effect on January 1, 2020, under the California Consumer Privacy Act of 2018 ("**CCPA**"). The CCPA, common U.S. privacy principles, security guidance promulgated by the Federal Trade Commission ("**FTC**") and industry best practices form the basis of this United States Policy (as defined below).

1.2 Background to United States Addendum/Policy

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

1.2.2 This United States 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 United States Addendum/Policy Part Of Employment Contract

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

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

1.3.3 This United States Policy seeks to provide each employee with a broad summary overview of the requirements under U.S. privacy and security laws and industry best practices, and an understanding of their impact on operational activities.

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

If you have information or become aware that a breach under the United States Policy, Global Data Protection Policy or otherwise under any applicable U.S. law has occurred within the Organisation, please report it immediately to the Data Protection Officer, details of the Data Protection Officer can be found in the Global Data Protection Policy.

2. OVERVIEW OF UNITED STATES DATA PRIVACY AND SECURITY LAW LANDSCAPE

2.1 United States Privacy and Security Law Overview

2.1.1 **CCPA**. The CCPA establishes a comprehensive legal framework to govern the collection and use of personal information, both online and offline, and provides privacy rights to California consumers, in effect becoming the *de facto* national standard for privacy law in the United States. The CCPA introduces legal risks and considerations for companies that collect information from California consumers (defined as a natural person who is a California resident), due to the law's expansive scope, broad definition of personal information, increased disclosure obligations, enhanced consumer rights, potential for statutory fines and, in the event of a security incident, the potential for consumer class action litigation**.** With regard to dealing with personal information of any California consumer, the Organisation as a covered "business" under the CCPA is subject to the following obligations and should note the following:

A. **Definition of "Personal Information"**: The CCPA defines "personal information" broadly to mean any information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. For examples of data elements that may be considered personal information and would be subject to the restrictions of the CCPA, please see **Appendix A**.

a. **Exclusions.** Note, certain types of information are excluded from the definition of personal information and the scope of the CCPA, including:

i. Publicly available information, which is information that is lawfully made available from federal, state, or local government records;

ii. Aggregate information, which is information relating to a group or category of consumers, from which individual consumer identities have been removed, that is not linked or reasonably linkable to any consumer or household, including via a device; and

iii. Deidentified information, which is information that cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular consumer, and that is subject to heightened technical and organizational safeguards by the business.

b. **Limited Exemptions**. In addition, the CCPA provides for a **limited exemption** for certain types of personal information typically collected in the business context. Until January 1, 2023, the following types of personal information will be excluded from most, but not all, of the provisions of the CCPA (please see the corresponding footnotes for more information as to which provisions of the CCPA these types of personal information are not excluded from):

i. **"Employee exception."** Any personal information collected by a business about a "natural person" in the course of the natural person acting as a job applicant to, employee of, owner of, director of, officer of, medical staff member of, or contractor of the business, but only to the extent that the information is used solely in the context of the person acting in that role. This also includes emergency contact information associated with such a person, as well as information necessary for the business to administer benefits, such as information about the employee's dependents and beneficiaries.[1]

ii. **"B2B Contact exception."** Any information that reflects a communication or transaction between a business and the employees of a third-party entity (as well as the controlling owners, directors, officers, and contractors of the third party) occurring within the context of the business providing or receiving a product or service to or from such third-party entity or in the context of conducting due diligence.[2]

B. **The "Sale" of Personal Information**: "Sell," "selling," "sale" or "sold" are defined broadly in the CCPA to mean selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information to another business or a third party for monetary or other valuable consideration.

a. The following types of disclosures do not constitute a "sale":

i. the consumer directs the disclosure or uses the business to intentionally interact with a third party;

ii. the disclosure is made to facilitate an opt-out request;

[1] This exception does not apply to the obligation to provide notice of data practices at or before the point of data collection nor to the liability for data breaches under the CCPA.

[2] This exception does not apply to the Right to Opt Out of "sales", nor to the liability for data breaches as under the CCPA.

iii. disclosures are made to “service providers” or “certified partners”; or

iv. disclosures made in the context of a merger or other qualifying corporate transactions.

b. Where a business does “sell” personal information, it must provide the ability for a consumer to opt-out of data “sales” to third parties. If the business has actual knowledge the consumer is under the age of 16, this reverses to a right to opt-*in*, and the business is prohibited from selling the personal information of the consumer under age 16 without prior affirmative opt-in consent. To be sure, it is important to correctly identify data sales in order to honor the consumer’s choice. However, it’s also important to identify data disclosures that are *not* data sales to avoid unnecessary opt-outs that may be administratively burdensome to execute or that have a negative impact on vital business functions.

c. In addition, an amendment to the CCPA imposes additional obligations on businesses that knowingly collect and sell personal information about consumers with whom the business does not have a direct relationship. These businesses that operate in the secondary data sales market must register as a “data broker” with the California Attorney General and provide contact information to be made available on the Attorney General’s website. Businesses are not considered “data brokers” to the extent that they are covered by certain state or federal laws, or if the business has a direct relationship with the consumer whose data it “sells.”

C. **Disclosure Obligations**: A business is required to make certain disclosures to consumers at or before the point of data collection, in its online privacy notice or on its website(s) and in any description of privacy rights targeted specifically to California residents. These disclosure obligations include:

a. Businesses must disclose what categories of personal information are collected about California consumers and the commercial or business purpose for which the personal information was collected;

b. Businesses must disclose what sources from whom they collect the personal information;

c. Businesses must disclose the categories of personal information that will be shared with third parties, as well as the categories of third parties with whom such personal information will be shared; and

d. Businesses must provide consumers with a description of their various rights provided by the CCPA and instructions on how to exercise those rights.

D. **Consumer Rights**:

a. The CCPA grants consumers with the following rights with respect to their personal information:

i. **Right to Access/Know**. The right to request the following information about the personal information a business has collected about the consumer in the last 12 months:

1. The categories and specific pieces of personal information collected;

2. The categories of sources of the personal information;

3. The purposes for collecting the personal information;

4. The categories of third parties with whom the personal information is shared;

5. The categories of personal information sold and the categories of buyers/recipients; and

6. The categories of personal information disclosed for a business purpose and the categories of recipients.

ii. **Right to Request Deletion**. The right to request the deletion or erasure of personal information a business has collected from the consumer.

iii. **Right to Opt Out**. The right to direct a business not to sell the consumer's personal information.

iv. **Right to Opt In**. The right of a consumer under the age of 16 to not have his or her personal information sold by a business that has actual knowledge the consumer is under 16 years of age without proper affirmative authorization or opt-in consent.

v. **Right Against Discrimination**. The CCPA also provides a Right Against Discrimination to ensure that a consumer is not penalized or retaliated against by the business for exercising her consumer rights.

These consumer rights are not absolute and can be limited when a specific set of exceptions apply.

b. Methods for consumers to submit consumer rights requests:

i. **Right to Access/Know/Deletion**. The business must provide two or more methods for a consumer to submit a consumer request under the Right to Access/Know and Right to Deletion, including a toll-free number, email address or online form. The business must verify the request and may need to gather additional information from the requesting consumer to ensure the consumer is authorized to submit the request, and/or to receive the information requested. The business must acknowledge receipt of the request within 10 business days and must respond within 45 calendar days of receipt of the request, though this period may be extended in certain circumstances. For requests to Access/Know, the business that receives a verifiable consumer request from a consumer to access personal information shall promptly take steps to disclose and deliver, free of charge to the consumer, the personal information required by the CCPA.

ii. **Right to Opt Out/Opt In**: The process to provide a mechanism for consumers to exercise their Rights to Opt Out / Rights to Opt In, and the business's required response to such a request, are notably distinct from the process to facilitate the consumer's Right to Access/Know or Right to Request Deletion. For example, a business that sells personal information must include a button or link called "Do Not Sell My Personal Information" on the homepage of the website or online service, in the privacy notice and within a mobile application (if applicable). The Organisation should act upon a request to Opt Out / Opt In no later than 15 business days from the date the business receives the request.

c. For information on how the Organisation handles consumer rights requests, see Section 3.5.

E. **Contracting Under the CCPA**: Many of the CCPA provisions concern the disclosure of personal information to vendors, contractors, partners, non-branded affiliates or any other entities or individuals ("**recipients**"). The CCPA raises different contracting considerations relating to data sharing, depending on the type of recipient, the purpose for which the personal information is shared, and the limitations imposed on the recipient's use of the personal information. The statute defines three main categories of recipients with whom the data may be shared:

a. **Service Provider**. A service provider is a for-profit, legal entity that receives personal information from a business for a business purpose and processes personal information on behalf of the business pursuant to a written contract that permits the service provider to retain, use or disclose the information only to perform specified services or as otherwise permitted by the CCPA.

b. **Certified Partner**. The CCPA creates a category of "persons"[3] who by definition are not "third parties" under the law. To qualify as a "certified partner," a person must receive personal information from a business for a business purpose pursuant to a written contract that prohibits the sale of personal information, prohibits the retention, use or disclosure of the information for any purpose other than providing the services specified in the contract, or for any purpose outside of the direct business relationship between the parties, and requires the person to explicitly certify that it understands these restrictions and will comply with them.

c. **Third Party**. A third party is any person who is not (i) the business itself or (ii) a certified partner. Third parties are generally recipients of personal information that are not subject to a written contract including specific restrictions on retention, use and disclosure enumerated in the CCPA.

Under the CCPA, disclosures made pursuant to a written contract properly structured to qualify the recipient of personal information as a service provider or certified partner do not constitute "sales" of personal information under the CCPA and are not subject to a consumer's right to opt out.

F. **Enforcement, Penalties and Private Right of Action**:

a. The CCPA grants the California Attorney General the power to enforce the CCPA by bringing actions against businesses who fail to comply with their obligations under the statute. If a business does not adequately correct areas of noncompliance with the law within 30 days of the California Attorney General's notice, the California Attorney General may impose specific sanctions including but not limited to an injunction and statutory civil penalties for failure to comply with the CCPA.

b. In addition, the CCPA permits a consumer the right to bring an individual cause of action or a class action against a business if their nonencrypted or nonredacted personal information is subject to an unauthorized access and exfiltration, theft or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information. It is essentially a cause of action against businesses that suffer data breaches. The private right of action under the CCPA provides for statutory damages. The consumer may also receive actual damages (in lieu of statutory damages if they are greater), injunctive or declaratory relief, and any other relief the court deems proper.

[3] "Person" means an individual, proprietorship, firm, partnership, joint venture, syndicate, business trust, company, corporation, limited liability company, association, committee, and any other organization or group of persons acting in concert. CCPA Section 1798.140(n).

2.1.2 **Common United States Privacy Principles**. There are common themes across privacy laws in the United States. In general, privacy laws in the United States do not expressly impose specific principles or legal bases related to the processing of personal information. Accordingly, there is no uniform view of how personal information should be processed. The FTC has promulgated fair information practice principles ("**FIPPs**") for the way in which online entities collect and use personal information and safeguards to assure that practices are fair and provide adequate information security:

(a) The "core" principles are: (i) Notice/Awareness; (ii) Choice/Consent; (iii) Access/Participation; and (iv) Integrity/Security.

(b) The FIPPs provide an indicator of how the FTC views how businesses should conduct themselves when processing personal information. The FTC has developed efforts to monitor industry self-regulation practices, provided guidance for developing information practices, and has used its authority under the FTC Act to enforce promises made by businesses in any of their public-facing materials, including their privacy notices.

(c) The principles, however, underly both federal and state laws, and continue to serve as a model for data privacy protections in developing areas and industries.

2.1.3 **Federal Trade Commission Guidance Regarding Data Security**. In respect to cybersecurity, the nature and scope of security obligations in the United States is still in development, but many laws mandate "reasonable and appropriate security measures." At the federal level, this requirement is found in some sector-specific statutes and regulations. In addition, the FTC has taken the position that this requirement applies broadly to all companies under its jurisdiction by means of the FTC Act, although this is disputed. FTC guidance advises entities to implement a "comprehensive security program that is reasonably designed to address security risks" and "protect the privacy, security, confidentiality, and integrity" of consumers' information.

(a) In a series of FTC enforcement actions, the FTC has asserted that these security programs have been required to address a wide range of potential risks, including:

i. employee training and management;

ii. secure software design, development and testing, including for default settings, access key and secret key management, and secure cloud storage;

iii. information systems, such as network and software design, information processing, storage, transmission, and disposal;

iv. review and assessment of as well as response to third-party security vulnerability reports; and

v. prevention and detection of as well as response to attacks, intrusions, or other system failures or vulnerabilities.

(b) Following the identification of security risks, FTC guidance indicates that it believes entities must also:

i. design and implement "reasonable safeguards" to control the identified risks;

ii. conduct regular testing of the effectiveness of key controls, systems and procedures, and evaluate and adjust information security programs based on the results of the testing;

iii. have a written information security policy;

iv. adequately train personnel to perform data security-related tasks and responsibilities;

v. ensure that third-party service providers implement reasonable security measures to protect personal information, such as through the use of contractual obligations;

vi. regularly monitor systems and assets to identify data security events and verify the effectiveness of protective measures;

vii. secure remote access;

viii. restrict access to data systems based on employee job functions;

ix. develop comprehensive password policies, addressing password complexity, safeguard against phishing threats; and

x. conduct vulnerability and penetration testing, security architecture reviews, code reviews, and other reasonable and appropriate assessments, audits, reviews or other tests to identify potential security failures and verify that access to devices and information is restricted consistent with user security settings.

3. U.S. PRIVACY PROGRAM FRAMEWORK

3.1 Introduction

In order to assist with complying with its CCPA obligations and U.S. data privacy and security industry best practices, the Organisation has implemented a privacy program as set out below.

3.2 Program Framework

The Organisation has created the United States Policy and the Global Data Protection Policy for its privacy program that acts as a foundation for the privacy program and establishes the purpose and scope of the program.

3.3 Governance, Oversight and Training

The United States Policy establishes who will oversee the program internally and serve as the primary contact for all questions related to the program. The Data Protection Officer and all employees handling personal information related to the program receive appropriate training to their job responsibilities.

3.4 Organisational Privacy Controls

The United States Policy and the Global Data Protection Policy establish guidelines for managing the Organisation's personal information processing activities, including how the Organisation creates and manages its personal information inventory, collects, uses, and shares personal information and notifies data subjects of this information.

3.5 Consumer Rights

The United States Policy and K&S' website privacy policy establish guidelines and a general policy for receiving, verifying, analyzing, recording and responding to consumer rights requests under the CCPA.

3.6 Marketing

K&S' marketing communication department sets out guidelines on how the Organisation develops and maintains its marketing strategy and materials. Please reach out to K&S' marketing communication department for more information.

3.7 Information Security Policy

The United States Policy establishes how the Organisation intends to maintain a secure network environment and to satisfy its legal, regulatory, contractual and ethical data security requirements, including further guidance on the Organisation's vendor due diligence and third party oversight procedures. Please refer to K&S' Information Security Policy.

3.8 Incident Response Policy & Plan

K&S' Data Breach Management Plan outlines the Organisation's general procedures for identifying, reporting, investigating, resolving and documenting suspected or actual incidents that may compromise the Organisation's systems or personal information.

Kulicke & Soffa

APPENDIX A

EXAMPLES OF CCPA PERSONAL INFORMATION

Category	Examples of Specific Pieces of Personal Information
Identifiers	Real name, alias, postal address, customer number, email address, unique personal identifier, account name, social security number, driver's license number, passport number, or other similar identifiers. A unique personal identifier is a persistent identifier that can be used to recognize a consumer, family or device over time and across different services (including a device ID, cookies, pixels, mobile ad identifiers, or other forms of persistent or probabilistic identifiers that can be used to recognize a particular consumer or device).
CA Customer Records Categories	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, debit card number, or any other financial information, medical information, or health insurance information.
Protected Classification Characteristics	Race, color, sex/gender, sexual orientation, gender identity, gender expression, age (date of birth), religion, national origin, disability (mental or physical), citizenship, legal status, marital status, medical condition, pregnancy, military or veteran status, and genetic information.
Commercial Information	Records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.
Biometric Information	An individual's physiological, biological or behavioral characteristics, including an individual's deoxyribonucleic acid (DNA), that can be used, singly or in combination with each other or with other identifying data, to establish individual identity. Biometric information includes, but is not limited to, imagery of the iris, retina, fingerprint, face, hand, palm, vein patterns, and voice recordings, from which an identifier template, such as a faceprint, a minutiae template, or a voiceprint, can be extracted, and keystroke patterns or rhythms, gait patterns or rhythms, and sleep, health, or exercise data that contain identifying information.
Internet or Network Information	Browsing history, search history, and information regarding a consumer's interaction with an Internet website, application, or advertisement.
Geolocation Data	This term is not defined in the CCPA, but likely includes any information that can be used to identify a consumer's precise or general physical location (e.g., GPS coordinates, Wi-Fi connection location).
Sensory Information	Audio, electronic, visual, thermal, olfactory, or similar information.
Professional or Employment Information	This term is not defined in the CCPA, but likely includes any information relating to a consumer's current, past or prospective employment or professional experience (e.g., job history, performance evaluations).
Education Information	Personal information from an educational record, which could include: a student's name, the names of the student's parent or other family members, the address of a student or student's family, a student's personal identifier (e.g., SSN, student number), other indirect identifiers of the student (e.g., date of birth, place of birth, mother's maiden name), other information that, alone or in combination, is linked or linkable to a specific student that would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify the student with reasonable certainty, or information requested by a person who the educational agency or institution reasonably believes knows the identity of the student to whom the education record relates. *See definition from FERPA, 20 U.S.C. Sec. 1232g, 34 C.F.R. Part 99.*

Other Personal Information	Other information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household.
Inferences	The derivation of information, data, assumptions, or conclusions from any of the above categories of personal information to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities and aptitudes.

APPENDIX B

ORGANIZATIONS

1. KULICKE AND SOFFA INDUSTRIES, INC.

2. KULICKE & SOFFA GLOBAL INVESTMENTS, INC

3. KULICKE & SOFFA FOREIGN INVESTMENTS, LLC

4. AMERICAN FINE WIRE LIMITED

5. K&S WORLDWIDE, INC.