GLOBAL DATA PROTECTION POLICY – ISRAEL ADDENDUM

KULICKE AND SOFFA (ISRAEL) LTD.

MICRO - SWISS LTD.

Kulicke & Soffa

GLOBAL DATA PROTECTION POLICY - ISRAEL ADDENDUM

KULICKE AND SOFFA (ISRAEL) LTD.
MICRO - SWISS LTD.

(collectively, the "**Organization**")

1. INTRODUCTION

1.1 Background to the Israeli protection of privacy law

1.1.1 Article 7 of the Basic Law: Human Dignity and Liberty, 5752 – 1992, establishes a constitutional right for privacy in Israel.

1.1.2 On a statutory level, Israeli law includes an omnibus privacy and data protection statute: the Protection of Privacy Law, 5741-1981 (the "**PPL**"). The PPL and Israeli law in general only protect the privacy of individuals. Corporations and other legal entities are not afforded privacy under Israeli law.

1.1.3 The Israeli Privacy Protection Authority (the "**Authority**"), a department within the Israeli Ministry of Justice, serves as the Israeli regulator in charge to administer and enforce the PPL. The Registrar of Databases (the "**Registrar**") is the regulatory authority under the PPL. The Registrar operates as a part of the Authority.

1.2 Background to Israel addendum

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

1.2.2 This Israel 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 Israel addendum is part of employment contract

1.3.1 All employees and agents of the Organization must strictly comply with this Israel Policy. For employees of the Organization, this Israel 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 Israel Policy from time to time. Any such amended 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 Israel Policy seeks to provide each employee with a summary overview of further key requirements of the PPL.

1.3.4 For detailed information on the obligations and exceptions under the PPL, you may refer to the PPL itself [Hebrew] as well as guidelines from the Israeli Privacy Protection Authority [Hebrew].

1.4 What to do if you are aware of or suspect a breach of the PPL

1.4.1 If you have information or become aware that a breach under the Israel Policy, Global Data Protection Policy or otherwise under the PPL has occurred within the Organization, please report it immediately to the Data Protection Officer. For further information as to reporting obligations of Severe Data Security Incidents under the PPL (as defined below), please refer to the Data Security section herein.

2. OVERVIEW OF PPL

2.1 The data protection obligations applicable to Personal Data

With regard to dealing with personal data of any individuals, the Organization and all employees are required to adhere to the following key data protection principles, as further described in this Israel Policy:

(a) Notice;

(b) Consent;

(c) Data Security;

(d) Right to review, amend and delete data;

(e) Legitimacy and proportionality;

(f) Database registration; and

(g) Cross-border transfer of personal data.

3. NOTICE

3.1 Introduction

3.1.1 Section 11 of the PPL provides that any request to receive personal data from an individual for the purpose of storing or using the data in a database - must be accompanied with a notice to such individual specifying the following:

(a) whether that individual is under a legal duty to provide that data or whether the provision of the data depends on that person's volition and consent;

(b) the purposes for which the data is requested; and

(c) to whom the data is to be transferred and the purposes of transfer.

3.2 Legal duty to provide Personal Data

3.2.1 Other than data required by employment and tax law, employees are not obligated by law to provide the Organization with their personal data and its provision is subject to their consent.

3.3 The purposes for which the Personal Data is requested

The details as to the purposes for which the personal data is requested are as detailed in the Global Data Protection Policy.

3.4 To whom the data is to be transferred and the purposes of transfer.

Details of transfer of personal data are as detailed in the Global Data Protection Policy.

4. CONSENT

4.1 Introduction

The PPL provides a list of circumstances which constitute an infringement of privacy, including:

(a) unlawful wiretapping;

(b) photographing an individual within private premises;

(c) publishing a photo of an individual in public if such publication may humiliate or disgrace him or her; and

(d) using data about the private matters of an individual, or delivering it to another, for a purpose other than for which it was originally collected.

4.2 Consent is a fundamental aspect of privacy under the PPL. Section 1 of the PPL provides that no person shall invade the privacy of an individual **without his or her consent**. Thus, by obtaining an individual's advance informed consent for collection and use of personal data, the intended use will not be considered as an infringement of privacy. There are no other legal bases under the PPL for collection and use of personal data, except where such collection and use are due to a specific legal requirement.

4.3 The PPL further provides that consent may be **explicit or implied**. Such consent must be "informed". While the term "informed" is not defined in the PPL, the acceptable meaning of this term is: a mindful decision made by an individual whether to provide consent or not, after being provided with all necessary information. The purpose of the Global Data Protection Policy and this Israel Policy is to provide such information.

4.4 The employer's collection and use of employees' personal data warrants elevated standards of disclosure and consent, as provided in the Global Data Protection Policy and this Israel Policy.

5. DATA SECURITY

5.1 Introduction

5.1.1 The Protection of Privacy Regulations (Data Security), 2017 [Hebrew] applies to all organizations, companies, and public agencies who own, manage, or maintain databases containing personal data in Israel (the "**Data Security Regulations**"). The Data Security Regulations create four tiers of databases, each subject to an escalating degree of information security requirements:

(a) databases maintained by individuals;

(b) databases subject to the basic level of data security (i.e., those that do not fall within any other category, and certain employee and HR data);

(c) databases subject to intermediate data security (i.e., those to which more than 10 people have access credentials and whose purpose includes making information available to other parties); and

(d) databases subject to a high level of data security (i.e., those whose purpose includes making information available to other parties, and with respect to which either more than 100 people have access credentials, or the number of data subjects is at least 100,000).

5.2 Information security measures

5.2.1 The Data Security Regulations require certain data security procedures that vary by database category and may include penetration testing, security incident assessments, risk

assessments, data breach notification, and monitoring of access to the database, as further described herein.

5.2.2 The Data Security Regulations require anyone who owns, manages or maintains a database containing personal data to implement, among other requirements, the following information security measures:

(a) maintain physical and environmental security controls;

(b) establish access credentials and manage those credentials on the extent necessary for users to perform their work;

(c) employ workers in database-related positions only if they have an appropriate level of clearance in relation to the database's degree of sensitivity and provide them training with respect to information security;

(d) maintain and document information security incidents; and

(e) keep records, documents, and decisions to demonstrate compliance with the Data Security Regulations.

5.2.3 The Data Security Regulations introduce additional requirements applicable to databases subject to the intermediate level of security, including:

(a) equipment brought in or taken out of the database's physical premises shall also be monitored;

(b) an extended data security protocol shall cover, among other issues, user authentication measures applicable to the database, backup procedures, access controls and periodic audits;

(c) a protocol shall be established for means of identification, frequency of password change and response to errors in access control;

(d) audit logs shall be maintained for at least two (2) years;

(e) either an internal or external audit shall be performed at least once in 24 months; and

(f) a backup and recovery plan shall be established.

5.2.4 The Data Security Regulations introduce additional requirements applicable to databases subject to the highest level of security, including:

(a) a risk assessment once every 18 months, using a qualified professional;

(b) penetration tests on the database’s computer systems once in 18 months; and

(c) security incidents shall be reviewed at least once every calendar quarter, and an assessment shall be made of the need to update security protocols.

5.3 Data security incidents

5.3.1 The Data Security Regulations require that the owner of a database document every event that raises concerns of a breach of the database’s integrity, unauthorized use thereof or deviation from authorization. The documentation should be based, to the greatest extent possible, on automated records.

5.3.2 The database owner is also required to establish instructions for handling different security incidents, according to the security incident’s severity and the information’s sensitivity level, including all necessary measures to be immediately taken at the event of a security incident.

5.3.3 The Data Security Regulations define the term "**Severe Data Security Incident**" as any of the following:

(a) in a database subject to a high level of data security – an incident involving the use of data from the database without authorization or in excess of authorization, or where the integrity of the data was compromised; or

(b) in a database subject to an intermediate level of data security – an incident involving the use of a material portion of the database without authorization or in excess of authorization, or where the integrity of a material portion of the database was compromised.

In case of such a Severe Data Security Incident, the database owner is required to immediately notify the Authority of the incident and the measures taken in response. Guidance issued by the Authority indicates that notification should be issued not later than within 72 hours of becoming aware of the Severe Data Security Incident. The Authority may instruct the database owner to provide such notice to the affected data subjects, at its discretion in accordance with the circumstances of the incident.

6. INDIVIDUALS' RIGHT TO REVIEW, AMEND AND DELETE DATA

Introduction

6.1 The PPL grants each individual a right to review the "Data" (as defined in Section 6.2 below) pertaining to him or her which is stored in a database. Any individual that wishes to review the data about him or her which is stored in a database, must submit a signed written request to the Organization or to Data Intermediaries or Data Processors which process such data for the Organization, pursuant to the Protection of Privacy Regulations (Conditions for Viewing Data and Procedures for Appealing Declined Requests to View), 5741-1981 [Hebrew]. The Organization must allow such individual to review the data pertaining to him or her within 30 days from receipt of the written request.

6.2 Pursuant to the PPL's definition of "Data", the PPL only grants an individual a right to review those items of stored Data which fall within the following categories: an individual's personality, marital or familial status, intimate affairs, health, financial status, professional qualifications, opinions and beliefs.

6.3 Under the PPL, a database owner (or holder – such as Data Intermediaries or Data Processors) may decline a person's request to review the data in various circumstances, the most relevant of which is where the delivery of data to the individual would violate of a privilege prescribed by statutory law or case-law, unless the person making the request is the beneficiary of the privilege (for instance, the privilege of data prepared for legal proceedings, or for an alternative dispute resolution process, have both been recognized by Israeli case-law). A database owner's notice to an individual declining his or her request to review the data must be provided to such individual within 21 days of from receipt of the request.

6.4 In addition, the PPL provides individuals with the right to request an amendment to or deletion of their personal data. If, upon review, a person finds that their personal data are inaccurate or incomplete, they may request that the data be amended or deleted.

7. THE PRINCIPLES OF LEGITIMACY AND PROPORTIONALITY

7.1 Introduction

Israeli case-law underscores that collection and processing of personal data must conform with the principles of legitimate-purpose and proportionality.

7.2 Legitimate purpose

7.2.1 The legitimacy principle requires that personal data be collected and processed only for essential purposes. For example, case law dealing with collection of employee data

interpreted such essential purposes where such collection and processing are necessary to safeguard the vital interests of the employer and prevent grave harm to these interests.

7.2.2 The Organization should take measures to ensure that personal data is used strictly for the legitimate purpose as provided in the Global Data Protection Policy.

7.3 Proportionality

7.3.1 The proportionality principle requires that the collection and processing of personal data be carried out in no greater scope, extent and degree than is necessary for the furtherance of the legitimate purpose.

7.3.2 For the purposes of reference and clarity, we will outline below the primary measures we recommend taking in order to comply with the proportionality principal. The Organization should ensure that:

(a) personal data not pertinent to the Organization or not necessary, is not collected or stored.

(b) data is accessible only to a limited number of individuals in the Organization, who are bound by proper confidentiality obligations.

(c) the personal data is purged once it has been handled, unless there is substantiated justification to archive it for future retrieval (such as to demonstrate that an employer has met its obligations under labor laws).

7.3.3 There are no privacy or data security obligations where the data cannot identify a person, such as where it was anonymized.

8. RETAINING A DATABASE WITH PERSONAL DATA

8.1 Database Registration

8.1.1 Database is defined in the PPL as a collection of data maintained in electronic form, excluding (a) a collection of data maintained for personal use rather than for business purposes; and (b) a collection that includes only names, addresses, and contact information, and which by itself does not create any characterization that infringes on the privacy of the persons whose data is included therein. This second exemption has been interpreted narrowly by the Authority, which has stated that a collection of names and email addresses does not fall within the exemption.

8.1.2 The PPL requires that certain databases be registered with the Registrar, which operates within the Authority. This general obligation is for registering any database that meets any one or more of the following criteria that may be relevant to the Organization: (a) it holds data about 10,000 persons or more; (b) it holds Sensitive Data (defined below); or (c) it includes data about people and the data was not provided by them, or on their behalf, or with their approval.

"**Sensitive Data**" is defined as data regarding the personality, intimate affairs, health, financial status, opinions, or beliefs of an individual.

8.1.3 Generally, the process for registering a database is primarily an administrative procedure, carried out by filling out a template application. The database registration system is database-driven and not owner-driven. Hence, if a database owner has several databases, it must register each database separately.

8.1.4 If the Organization already registered a database pertaining to employees with the Registrar, the existing database registration may need to be updated to accurately reflect the contemplated uses.

8.2 Database Owner vs. Database Holder

The PPL makes a distinction between a database owner (similar to a controller), which has the primary title and interest in the database (the Organization), and a database holder, which is a person or entity that merely possesses the database and is permitted to use it (such as a processor on behalf of the owner or Data Intermediaries). A database registration application must include a list of all legal entities which are considered as holders of such database. Both the database owner and the database holders are obligated to meet all data security requirements as provided in the Data Security Regulations.

9. CROSS-BORDER TRANSFER OF PERSONAL DATA

9.1 The Protection of Privacy Regulations (Transfer of Data to Databases Abroad) 5762 – 2001 (the "**Data Transfer Regulations**") govern cross-border transfer of personal data from Israel.

9.2 No such transfer is allowed, unless the law of the jurisdiction to where the data is transferred for use or processing ensures a level of privacy protection no lesser than the level provided under Israeli law, and such law mandates, among others, the following principles:

(a) Data is collected and processed in a fair and lawful manner;

(b) Data is processed only for the purpose for which it was collected;

(c) Collected data is kept accurate and up-to-date;

(d) Individuals are granted a right to review the data stored about them; and

(e) Adequate security measures to safeguard the data are required.

There is no official “whitelist” of countries which have been recognized by Israel as satisfying these requirements.

9.3 Regulation 2 of the Data Transfer Regulations provides certain “safe-harbor” exceptions which permit cross-border transfer of personal data, including:

(a) the individual to whom the data pertains has consented to the transfer;

(b) the data is transferred to a corporation under the control of the Organization, and that corporation has guaranteed the protection of privacy after the transfer;

(c) the data is transferred to a person bound by an agreement with the Organization, to comply with the same conditions for possession and use of the personal data which apply to a database in Israel, mutatis mutandis; or

(d) the data is transferred for use and processing in a country, which is either: a party to the European Convention for the Protection of Individuals with Regard to Automatic Processing of Sensitive Data; or receives data from Member States of the European Community, under the same terms of acceptance provided in the European Data Protection Directive.

9.4 In addition to the above requirements, the Data Transfer Regulations also require that the Organization receive a binding statement from the receiving entity, according to which such entity undertakes to implement adequate measures to ensure the privacy of the data, and not to transfer the personal data to any other person, whether in the same jurisdiction or elsewhere.