AUO'S POLICY ON DATA PROTECTION AND PRIVACY OF PERSONAL DATA

AUO'S POLICY ON DATA PROTECTION AND PRIVACY OF PERSONAL DATA

PURPOSE:

This Policy sets forth how AUO will manage the Personal Data that it collects in the normal course of business and constitutes integral parts of AUO's internal control and risk/compliance management system.

SCOPE:

This Policy's scope of application encompasses AUO Corporation, all branch offices, subsidiaries, and affiliates of AUO Corporation (collectively "AUO" or the "Group"), and their respective suppliers, service providers, consultants, contractors, advisors, and vendors. Specifically, this Policy applies to:

(a) all individuals who provide Personal Data to AUO, such as associates, job applicants, contingent workers, interns, retirees, contractors, customers, business partners, shareholders, and others;

(b) all locations where AUO operates, even where local regulations do not exist; and

(c) all methods of contact, including in person, written, via the Internet, direct mail, telephone, or facsimile.

This Policy is designed to inform all employees about their obligations to protect the privacy of all individuals who work for or deal with AUO and the security of their Personal Data. This Policy sets forth AUO's overall guidelines for dealing with Personal Data, and AUO will continue to evaluate its policies to ensure compliance with applicable laws and make adjustments when necessary.

POLICY:

This Policy describes the Group's standard global procedure governing access to and use of Personal Data across borders. As part of this Policy, the Group will comply in all material respects with the privacy laws, rules, and regulations that may apply to the Group, its employee, or its customers in those countries where the Group has operations.

AUO has designated the Legal Office of AUO Corporation ("Legal Office") as the central unit responsible for addressing group-wide privacy-related matters. For local operations, AUO has designated specific personnel (such as Data Protection Officers ("DPOs") or human resources managers) to oversee privacy-related matters in accordance with local laws and regulations and to act as the point of contact to whom employees can reach out in case of any privacy issues or concerns. Any questions or issues regarding this Policy can be directed to the local DPOs or human resources managers or escalated to the Legal Office.

DEFINITIONS:

Controller	Refers to AUO and its authorized third parties, which determine the purposes and means of processing of Personal Data.
Data Subject	Refers to any employee or third person (e.g., consultant or independent contractor) who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his or her physical, physiological, mental, economic, cultural or social identity.
General Business Purpose	Defined as the Processing of Personal Data for any activity related to the commercial operations of the Group's worldwide organization. This could include, but is not limited to, its sales, marketing and research and development operations; protecting intellectual property; the provisions of services; internal operations; information technology and general employment matters, including recruitment both internally and externally. Data processing for General Business Purposes includes, but is not limited to, publishing global directories, maintaining files, payroll processing, managing benefit and medical plans, conducting performance reviews, and intra-group communications.
Personal Data	Defined as any information related to an identified or an identifiable person. For example, a Data Subject's name, date of birth, photograph, video footage, home address, e-mail address, telephone number, location data, or government-issued identification numbers would constitute Personal Data. Other information such as Internet Protocol (IP) addresses and mobile phones' advertising identifiers would also constitute Personal Data to the extent that it can identify a certain individual.
Processor	Defined as a natural or legal person, or any other entity that processes Personal Data on behalf of the Controller and under its control. In this context, a processor may be a payroll preparation firm that works on behalf of AUO and under its control. The Group requires Processors to protect the privacy, confidentiality and security of Personal Data.
Processing	Defined as any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, storage, adaption or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.
Pseudonymize / Pseudonymization	Defined as the Processing of Personal Data in such a manner that the Personal Data can no longer be attributed to a specific Data Subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the Personal Data are not attributed to the Data Subject.
Sensitive Data	Defined as a subset of Personal Data, and varies in different jurisdictions. Sensitive Data usually refers to any Personal Data pertaining to racial or ethnic origins, political opinions, religious or philosophical beliefs, or trade union membership or the Data Subject's

	genetic data, biometric data, or data concerning health, sex life, sexual orientation, or criminal history.
Third Party	Defined as any natural or legal person, public authority, agency or any other entity other than the Data Subject, the Controller, the Processor and the persons who, under the direct authority of the Controller or the Processor, are authorized to process the Personal Data.

PROCEDURE:

Use of Personal Data

In the course of day-to-day business operations, authorized individuals within the Group may from time-to-time utilize and/or transfer Personal Data among various AUO worldwide locations. These transfers of Personal Data are necessary in order to carry out the Group's General Business Purposes.

Specifically, Personal Data may be used as follows:

a. To identify a Data Subject personally;

b. To communicate with a Data Subject;

c. To comply with human resource requirements;

d. To comply with government regulations;

e. To provide benefits; and

f. To manage the business.

Integrity of Personal Data

The Group will take reasonable steps to ensure that Personal Data and Sensitive Data are:

a. Obtained, where possible, directly from the Data Subject to whom the Personal Data relates and from a source other than the Data Subject if permitted by any applicable law;

b. Obtained and processed fairly and lawfully by the Group for General Business Purposes;

c. Relevant to and no more revealing than is necessary for General Business Purposes; and

d. Kept up-to-date to maintain data accuracy, while data is under the control of the Group, and kept only for so long as is reasonably necessary to fulfill the General Business Purposes for which such data is collected or if the Data Subject withdraws his/her consent, whichever occurs first.

Notice

The Group informs Data Subjects about the purposes for which Personal Data is collected and used. In certain situations, Personal Data may be rendered anonymous so that the Data Subjects are irrevocably de-identified. For Personal Data to be considered as anonymized, it needs to be stripped from any information that could link it back to the Data Subject (even in the cases where the data is combined with other data sources). After being anonymized, the data shall not be considered as Personal Data anymore.

If the Personal Data is provided to Processors without them having access to the name of the Data Subject, we would normally refer to it as pseudonymized data. In some jurisdictions, Data Subjects do not need to be notified of the processing of pseudonymized data depending on applicable laws.

Access to Personal Data

The Group takes steps to make sure that the Personal Data it uses is correct. The Group will allow Data Subjects reasonable access to Personal Data about themselves during normal working hours and upon reasonable request, and will be allowed to update, complete, and/or correct any inaccurate, misleading, or incomplete information.

Procedure for Accessing Personal Data

Questions about Personal Data and/or authorization to access such Personal Data are to be directed to local DPOs or human resources managers. Unauthorized access may be grounds for disciplinary actions, including but not limited to termination of relevant contracts or cooperation.

Group-wide Risk Management

AUO has established strategies and processes to respond to group-wide systematic risks in accordance with the risk management standards and guidelines of ISO 31000. AUO's risk management mechanisms consist of identification, analysis, and evaluation processes. The risk scope covers financial, strategic, operational, and disaster management aspects. The protection of privacy and Personal Data is an integral part of AUO's operational risk/compliance management structures. AUO conducts quarterly human right risk assessments, aiming at eight major human right issues, including Personal Data risk.

Security of Personal Data

The Group will implement appropriate security measures to protect Personal Data from loss, misuse, unauthorized access, disclosure, alteration and destruction.

Transfer of Personal Data

Subject to this Policy, the Group may from time-to-time transfer Personal Data within and between its various worldwide locations for General Business Purposes, in compliance with country of origin regulations and this Policy.

The Group's personnel, outside firms and consultants who receive Personal Data may be located in the Data Subject's home country, or any other country in which the Group or its affiliates do

business. Therefore, Personal Data may be transferred to any country in the world where the Group does business, and where the privacy laws may be more or less protective than the privacy laws where the Data Subjects live or work.

Choice

To the extent permitted by applicable laws, any employee whose Personal Data is to be transferred to Third Parties as described in this Policy may choose not have his or her Personal Data transferred. The Group should inform Data Subjects choose not have their Personal Data transferred of the impact such choice will have on their rights and interests within the Group (e.g., inability to process benefits or payroll data in a timely or appropriate fashion). Unless otherwise provided by applicable laws, the Group may transfer Personal Data to a Third Party for the following purposes without obtaining consent from a Data Subject:

a. Meeting applicable legal requirements; and

b. Permitting the legitimate interests of the Group in making promotions, appointments, preparing succession planning and other employment decisions.

Accountability

The Group expects its employees, suppliers, service providers, consultants, contractors, advisors and vendors to maintain the trust placed in the Group by those Data Subjects who provide Personal Data to the Group and to follow the same data protection practices set forth under this Policy. The Group may periodically audit privacy compliance of its employees, suppliers, service providers, consultants, contractors, advisors, and vendors.

Procedure for Inquiries, Complaints and Opt-Out

A Data Subject may contact local DPOs or human resources managers or the Legal Office with inquiries or complaints regarding the Group's processing of Personal Data or to opt out of the transfer of Personal Data (if applicable).

Enforcement

The Group uses a self-assessment approach to assure compliance with this Policy and periodically verifies that the policy is accurate, comprehensive for the information intended to be covered, prominently displayed, completely implemented and accessible. The Group encourages interested persons to raise any concerns using the contact information provided and we will investigate and attempt to resolve any complaints and disputes regarding use and disclosure of Personal Data in accordance with this Policy.

Audits

AUO has established an internal control and audit system. AUO's internal Auditing Administration Division has included the compliance with this Policy in its audit scope, conducts internal audits on an irregular basis according to its annual audit plan, and reports the audit results to the Audit Committee and the Board of Directors.

AUO also conducts on-site audits, document reviews, and employee reviews in accordance with the audit standards of the RBA (Responsible Business Alliance) Code of Conduct so as to ensure that no human right violations occurred (including commitment to privacy protection). To further ensure that AUO's privacy policies are consistent with global standards, AUO also engages independent external auditors to audit its privacy protection arrangements and procedures.

Disciplinary Actions

The Group adopts a zero-tolerance policy against data breach. Improper or unauthorized access, use, disclosure, alteration, destruction or loss of Personal Data will result in disciplinary actions, including but not limited to termination of relevant contracts or cooperation.

Amendments

This Policy may be amended from time to time. Revisions will be posted on AUO's website.

Inquiries

Any questions about this Policy can be directed to local DPOs or human resources managers or escalated to the Legal Office.