ASAHI NETWORKS PHILS., INC.
PRIVACY POLICY

A. PRIVACY STATEMENT

As a globally-recognized organization, Asahi Networks Phils., Inc. ("Asahi") takes the privacy rights of individuals seriously. As such, we always protect and secure the personal data we collect and process in compliance with Republic Act No. 10173, otherwise known as the Data Privacy Act of 2012 ("Data Privacy Act"), its corresponding Implementing Rules and Procedures ("IRR"), and the existing Memorandum Circulars and Advisories issued by the National Privacy Commission ("NPC").

B. SCOPE

1. This **document** provides our policy in relation to our personal data processing activities in accordance the Data Privacy Act, its IRR, and all related issuances of the NPC.

2. We may amend and/or modify this policy from time to time to reflect changes in how we process your data and to comply with developments in data privacy regulation subject to reasonable notice and consent, where applicable.

3. This **policy** applies to all of Asahi's personal data processing activities including, but not limited to, the collection, use, storage, sharing and disposal of all personal data about our employees, subcontractors, and individuals with whom we work with as representatives of our affiliates, partners, suppliers and customers.

C. COLLECTION AND USE OF PERSONAL DATA

1. SCOPE AND PURPOSE OF PERSONAL DATA PROCESSING

As a business process outsourcing company, we provide payroll management, corporate registration, and regulatory compliance and reporting services for various corporate clients. In the provision of such services, we receive and process personal data about our clients' employees, including their directors, officers, and/or agents. We process such data strictly for purposes of providing outsourced services and in accordance with the instructions of our clients. We also ensure that the data we receive from clients bear the consent of the data subjects from such data is originally collected. Some of the personal data we process include:

a. Employee name, address, tax identification number and birthdate;
b. Name of incorporator, address, nationality, passport details, and equity holdings;
c. Name of directors, address, nationality, passport details and equity holdings;
d. Name of officers, position, address, nationality, government identification, and tax identification number; and
e. Name of shareholders, nationality, government identification, and tax identification number.

We also collect and process the personal data of our employees for Administrative and Human Resource Development purposes as well as in compliance to applicable laws, rules and regulations covering government employees, including, but not limited to:

a. Maintenance of employee database for Identity verification procedures, internal security and access protocols, and regulatory compliance;
b. Pre-qualification and post-qualification assessments
c. Processing of various contracts, certificates and documents evidencing employment/engagement with ANP;
d. Processing and grant of employment compensation and corporate benefits, including payroll and loan management, Health Maintenance Organization ("HMO") and corporate loans;
e. Development and implementation of employee learning training, and welfare programs, including workplace performance and compatibility testing;
f. Maintenance of employee performance metrics as well as attendance records;
g. Compliance with government and regulatory requirements such as Bureau of Internal Revenue ("BIR"), Department of Labor and Employment ("DOLE"), SSS, PhilHealth, and Pag-IBIG reportorial requirements, business, and occupational permits, and licenses as well as other National Government and Local Government Unit (LGU) compliance requirements; and
h. For the protection of lawful rights and interests of the organization in internal quasi-judicial and judicial proceedings, or the establishment, exercise or defense of legal claims against prospectively malfeasant employees.

2. HOW WE COLLECT AND PROCESS PERSONAL DATA

We collect both electronic and paper-based personal data directly from our employees and clients through physical forms as well as through our company-licensed work productivity software and e-mail platform.

D. THE RIGHTS OF DATA SUBJECTS

Asahi fully recognizes that the data subjects involved in our personal data processing activities are accorded the following privacy rights:

- **Right to be informed**

They have the right to demand and be informed of the details about the type of personal data, the purpose of processing, and how they are being processed by Asahi, including its sources, recipients, methods, disclosures to third parties and their identities, automated processes, manner of storage, period of retention, manner of disposal and any changes to such processing activities before the same is undertaken.

- **Right to access**

They have the right to have reasonable access to their personal data, sensitive or otherwise, upon demand. They have the right to review and amend their personal data processed by the Asahi in case there are errors.

- **Right to dispute**

They have the right to dispute inaccuracy or error in personal data processed by Asahi.

- **Right to object**

They have the right to reject further processing of their personal data, including the right to suspend, withdraw, and remove their personal data in possession of ASAHI which are falsely collected or unlawfully processed.

E. POLICY ON THE COLLECTION AND USE OF PERSONAL DATA

In relation to the rights of Data Subjects, it is Asahi's policy to:

1. Ensure that our employees and our clients' employees, incorporators, directors and/or officers are fully and adequately informed of their privacy rights;

2. Ensure that they are fully and adequately informed of all processing activities performed by the Asahi with respect to their personal data;

3. Ensure that their consent is obtained where necessary prior to the processing of their personal data or within reasonable time thereafter. Where consent is not required, we will, nonetheless, endeavor to fully and adequately inform our members of the bases of such processing;

4. Ensure that they have the facility to reasonably access, review and amend their personal data and to request for copies thereof in a commonly portable format;

5. Ensure that they have the facility to: dispute any inaccuracy or error in their personal data, object to any changes in the manner and purpose by which they are processed, withdraw consent where applicable, and to suspend, withdraw, block, destroy, or remove any unnecessary, falsely collected or unlawfully processed personal data;

6. Ensure that such personal data are proportional, necessary and limited to the declared, specified and legitimate purpose of the processing;

7. Ensure that such personal data are retained for only a limited period or until the lawful purpose of the processing has been achieved;

8. Ensure that such personal data are destroyed or disposed of in a secure manner;

9. Ensure that they have the facility to lodge complaints to the IBP relating to any violations to their rights as data subjects and that such complaints are adequately and timely addressed.

F. DATA PROTECTION OFFICER

Asahi takes data protection seriously and has appointed a Data Protection Officer ("DPO") tasked to monitor compliance with any and all applicable foreign and/or local data privacy laws, rules, and regulations.

Should you have any concerns regarding our privacy practices and policies, you may reach our DPO through the following contact information:

Data Privacy Officer	
E-mail	stanaka@asahinet.ph
Office Address	44th Floor AIA Tower, 8767 Paseo de Roxas, 1226 Makati City, Philippines

G. PERSONAL DATA SECURITY POLICY

1. STORAGE OF AND ACCESS TO PERSONAL DATA

We ensure that all personal data stored by the organization, whether in manual or electronic form, are kept in secure areas with appropriate physical, technical and organizational security measures and accessed in accordance with the data security standards of the organization.

We adopt appropriate data collection, storage and processing practices and security measures to protect against unauthorized access, alteration, disclosure or destruction of your personal data, username, password, transaction information and

data stored and processed by the IBP, including appropriate encryption tools, firewalls and security incident management systems and procedures.

Transfers of personal data internally and externally shall only be made in accordance with strict security protocols and under modes of transfer compliant to the requirements and standards of the Data Privacy Act.

We also ensure that only authorized individuals within the organization shall be allowed to process personal data.

2. RETENTION AND DISPOSAL OF PERSONAL DATA

We ensure that personal data is only retained for a limited period or until the lawful and legitimate purpose of the processing is achieved. To that effect, we have established procedures for securely disposing files that contain personal data whether the same is stored on paper, film, optical or magnetic media, personal data stored offsite, and computer equipment.

3. MANAGEMENT OF THIRD-PARTY RISKS

a. PERSONAL INFORMATION PROCESSORS

Where any processing of personal data is outsourced to a third-party processor, Asahi will make sure that such third party shall be covered by the appropriate contracts that will enforce adequate data security standards under terms and conditions compliant with the requirements of both local and/or foreign law, where necessary.

b. PERSONAL INFORMATION CONTROLLERS

Asahi shall ensure that any disclosures or transfers of personal data to controllers shall be governed by legally-compliant data sharing agreements and in accordance with the rights of data subjects. Data subjects shall be duly informed and consent from them obtained, where applicable, before such data sharing activities are performed.

Apart from this, we do not sell or disclose your personal data to third parties unless you allow us to; when we are legally required to do so; or if such action is necessary to protect, defend and/or enforce our rights, property or the personal safety of our members and other individuals.

4. PERSONAL DATA BREACH

Personal Data Breach refers to a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored, or otherwise processed. Personal Data Breaches shall be subject to notification and remediation requirements.

5. HUMAN RESOURCE POLICY

Asahi requires its employees to undergo periodic and mandatory training privacy and data protection in general and in areas reflecting job-specific content. Likewise, it will ensure that all employees, representatives, and agents exposed to personal data pursuant to their function are adequately bound by strict confidentiality.