CHRISTIANI & NIELSEN

Personal Data Protection Policy
Christiani & Nielsen (Thai) Public Company Limited

Christiani & Nielsen (Thai) Public Company Limited and its Subsidiaries (collectively referred to as the "Company") recognize the importance of personal data protection as part of social responsibility, good corporate governance, and legal compliance. The Company believes that data privacy of its individual stakeholders (employees, shareholders, clients, business partners, suppliers, and visitors, etc.), involved in any area of the Company's business operations, is important and should be treated with utmost care. As such, the Company shall ensure that such individual's personal data is protected in accordance with application laws and regulations.

In light of the above, the Company has issued this Personal **Data Protection Policy** (the "Policy"), which adheres to the Personal Data Protection Act, B.E. 2562 (2019) (the "PDPA") in order to prescribe the Company's process of data collection, use, and disclosure, and other rights of the Data Subjects (as defined below).

The purpose of this Policy is to provide the appropriate framework for handling Personal Data (as defined below) and to ensure that there are sufficient security measures in place to protect and secure Personal Data which the Company is collecting, using, and disclosing in accordance with the PDPA and any related regulations thereof.

The Company may, from time to time, update this Policy to ensure that it is current and consistent with current events, future developments, industry trends, risk management, and/or any changes in legal or regulatory requirements.

1. Objective and Scope

1.1 This Policy is issued to ensure that the Company's business operations are carried out in compliance with the PDPA and relevant laws and regulations and also meet international standards in relation to protection of Personal Data.

1.2 This Policy applies to all directors, executives and staff, and extended to all business dealings in all jurisdictions within which the Company operates.

1.3 This Policy is considered as part of the Company's working regulations, with which the Company's employees must strictly comply.

2. Definitions

- **"The Company"** means Christiani & Nielsen (Thai) Public Company Limited and its Subsidiaries.
- **"Subsidiaries"** means the Company's subsidiaries and associated companies as listed on the Company website under Group Corporate Structures.
- **"Data Controller"** means the Company.
- **"Data Subject"** means an individual who is the owner of the Personal Data which is collected, used, or disclosed, including but not limited to employees, customers, shareholders, trading partners, service providers and interested parties.
- **"Data Processor"** means a person who operates any collection, use, or disclosure of Personal Data as per an instruction of or on behalf of the Data Controller.

- **"Personal Data"** means any information relating to a person which enables the identification of such a person, whether directly or indirectly, but not including the information of deceased persons in particular.
- **"Sensitive Personal Data"** means any information relating to a particular person which is sensitive and presents significant risks to the person's fundamental rights and freedoms, including data regarding racial or ethnic origin, political opinions, cults, religious or philosophical beliefs, sexual behavior, criminal records, health data, disabilities, trade union information, genetic data, biometric data, or any data which may affect the Data Subject in the same manner, as prescribed by the Personal Data Protection Committee.
- **"Data Protection Officer (DPO)"** means an officer who is responsible for advising, overseeing, and monitoring compliance with the PDPA, including coordinating and cooperating with the Office of the Personal Data Protection Committee on the Company's issues in relation to the collection, use, or disclosure of Personal Data, with other duties which may be required by the PDPA.
- **"Personal Data Protection Committee"** means the regulatory committee appointed under the PDPA, in charge of the duties and authorities to govern, issue criteria or measures, or provide any other guidance as prescribed by the PDPA.

3. Collection/use of Personal Data

The Company shall collect Personal Data to the extent necessary for the purpose and scope notified to the Data Subject before or at the time of collection.

3.1 Collection of personal Data

The Company shall ensure that it complies with the following guidelines when collecting Personal Data from a Data Subject:

3.1.1 Before collection of Personal Data, the Company shall consider the following:

- whether the Personal Data that will be collected by the Company is necessary for the purpose of the Company's business operations; and
- whether the purpose of the collection, use, or disclosure of the Personal Data fails within the legal exemptions that allow the Company to collect, use or disclose Personal Data without requiring consent from the Data Subject.

If the answer to any of the above is negative, the Company must obtain the consent of the Data Subject or if that is not possible, then the Company shall avoid collecting such Personal Data altogether. If such personal data was collected prior to the effective date of this policy, the company must destroy such personal data in accordance with Article 10 of this policy.

3.1.2 Before or at the time of the first collection of the Personal Data from a Data Subject, the Company must notify the Data Subject of the following details:

- Purpose of collecting Personal Data, including notification of the potential consequences if the Data Subject fails to provide such Personal Data;
- Notification of cases in which the Data Subject is required to provide his/her Personal Data in order to comply with law or contract, or where it is required to provide the Personal Data in order to enter into a contract, including notification of the possible consequences if the Data Subject does not provide such Personal Data;
- The personal data will be collected and retained for the period prescribed by law.
- The categories of individuals or entities to whom or which the collected Personal Data may be disclosed;
- The information, address, and contact channel details of the Company, as the Data Controller; and
- The rights of the Data Subject as mentioned below.

3.1.3 If it becomes necessary to change the purpose for which the Personal Data is processed, unless it is a case where the consent from the Data Subject is not required by law, the Data Subject must be informed of the new purpose, and the Company must obtain consent from the Data Subject, before any processing occurs.

3.2 Methods for collection/use of Personal Data

3.2.1 Collection and/or use of Personal Data that does not require the data subject's consent:

(1) The Company may collect and/or use non-sensitive Personal Data without obtaining consent from the data subject if the purpose of the collection and/or use falls within any of the purposes listed in Article 6 of this Policy and/or any other legitimate grounds permitted by the PDPA and/or relevant laws.

(2) The Company may collect and/or use Sensitive Personal Data without the Data Subject's consent if the purpose of the collection and/or use falls within the purposes permitted by the PDPA and/or relevant laws.

3.2.2 Collection and/or use of Personal Data that requires consent from the Data Subject:

If the Personal Data that the Company wishes to obtain from a Data Subject does not fall within the purposes mentioned in Article 3.2.1 above, the Company must obtain explicit consent from the Data Subject before collecting and/or using the Personal Data (unless consent cannot be obtained due to the nature of circumstance).

(1) Collection/use of Personal Data on paper:
In collecting Personal Data in paper format, the Company shall prepare a consent form to obtain consent from the Data Subject.

(2) Electronic collection/use of Personal Data:
In the case of collecting/using Personal Data in electronic format, the Company will prepare a consent document to be used for obtaining consent with no pre-answered (i.e., not set a default check in the message box that the Data Subject can select only to confirm or accept to any conditions).

In the collection/use of the Personal Data, the Company must ensure that consent is freely given on a voluntary basis by the Data Subject. The Company shall ensure that performance of a contract, including the provision of a service, will not be conditional on consent to the processing of Personal Data that is not necessary for the performance of that contract.

3.2.3 Records of the Collected Personal Data

The Company shall keep and maintain a record of the Personal Data processing activities (“ROPA”) which documents category of collected or used Personal Data, the purpose of collection of Personal Data, and the retention period of Personal Data which the Company has collected, used, and/or disclosed. The Company must amend or update such records on a regular basis to ensure that they are accurate and complete at all times.

The ROPA of each Department shall be maintained by the Department Head and the DPO.

4. Use of personal Data

The Company shall operate in accordance with the following principles and guidelines in using any Personal Data that it collects:

4.1 Personal Data may only be used for the specific purposes disclosed to the Data Subject when the data is collected.
4.2 Collected Personal Data that does not require consent may only be used for the specific purposes as mentioned in Article 3.2.1.
4.3 The Company shall keep record of the use of collected Personal Data as a part of the Company's ROPA.
4.4 The Company shall establish the conditions and methods for accessing Personal Data that it has collected for use or disclosure in accordance with the purposes for which the Data Subject has been informed.

5. Sources of Personal Data

The Company may collect the Personal Data from the following sources:

5.1 Personal Data received directly from the Data Subject.
5.2 Personal Data received from the Company's Subsidiaries.
5.3 Personal Data received from a third party such as agents, service providers and/or trading partners.
5.4 Personal Data collected from visiting websites such as name of the internet user and IP address, date and time of visiting the website, websites that are visited, address of the website which is directly connected with the Company's address.
5.5 Personal Data which can be collected from the public and non-public records that the Company has the right to collect as per the law.
5.6 Personal Data obtained from government organizations or authorized agencies.

6. Purpose of Collecting and Use of Personal Data

6.1 The Company shall collect or use Personal Data for the purposes or activities such as the procurement process, contracts execution, financial transactions, company activities, collaborations or improvement of the Company's processes, database preparation, process analysis and development, and/or any other purposes that are in compliance with the legal obligations or regulations to which the Company is subject. The Company shall retain and use the Personal Data as long as necessary only for the above-mentioned purposes, or as prescribed by laws.
6.2 Personal Data of employees, consultants, contractors, applicants, and/or temporary staff may be used for the following purposes; employment contract, social security, taxation, insurance, medical treatment and health records, performance evaluation, payroll, educational background, criminal records (only for some positions), financial records (only for some positions), and/or personal profiles for job applications.
6.3 Personal Data of clients, suppliers, business partners, shareholders, lenders, bondholders, warrant holders and/or investors may be used for the following purposes:
- Business transactions and related activities, research and development, marketing, PR, advertisement, CSR activities.
- Improving service and efficiency.
- Accepting complaints from clients and stakeholders.

- Communicating with the relevant stakeholders either through phone, text messages, e-mail, postal mail, and other communication channels; sending notifications, verifying client and stakeholder's accounts, survey and questionnaires.
- Verifying the relevant stakeholder's information in compliance with laws and regulations.

6.4 If the Company hires Data Processors who are external service providers such as law firms, insurers, hospitals, IT service providers, and so on, the Company must ensure that such Data Processors treat Personal Data as confidential. They are not permitted to use Personal Data for any purpose other than those specified by the Company.

6.5 The Company shall not use Personal Data for purposes other than those previously shared with the Data Subject except when:

a. The Data Subject has been informed of such a new purpose, and prior consent is obtained;
b. It is necessary for the Company to comply with the PDPA and/or other laws.

7. Disclosure of Personal Data

The Company shall not disclose Personal Data of the Data Subject without consent from the Data Subject and shall disclose it solely for the above-mentioned purposes. However, for the benefit of Company operations and/or the provision of services to the Data Subject, the Company may disclose Personal Data to its Subsidiaries, Data Processors or other required persons, domestically and internationally. The Company shall ensure that the aforementioned individuals treat the Personal Data as confidential and not use the Personal Data for purposes other than which are agreed upon.

The Company may disclose Personal Data of the Data Subject as required by laws and regulations, such as disclosing it to government agencies, state enterprises, and/or regulators. Further, the Company may disclose Personal Data by virtue of laws, such as requests for the purposes of litigation or prosecution, or requests made by the private sector or other persons involved in legal proceedings.

8. Direction of Personal Data Protection

The Company shall establish Personal Data security measures in accordance with applicable laws, regulations, rules, and guidelines for employees and other relevant persons. The Company shall promote and encourage employees to learn about and recognize their duties and responsibilities related to the collection, storage, use and disclosure of Personal Data. All employees are required to follow this Policy and all guidelines regarding Personal Data protection for the Company to be in full compliance with the PDPA.

The Company's measures to protect Personal Data are as follows:

8.1 The right to access, use, disclose, and process Personal Data is restricted to the specific person (s) only. Personal Identification must be verified to access Personal Data.

8.2 If Personal Data is transferred to a foreign country or to an external database, the Company must ensure that the data controller at the destination secure the Personal Data. The level of data protection must be the same or better than the level in this policy.

8.3 Papers that contain an employee's Personal Data are prohibited from being reused. They will be destroyed once the employment ends or after expiry of the specific legally allowed period, except in case where there are other pending legal matters.

8.4 If there is a violation of this policy's data security measures, or a leak of Personal Data, the Company shall notify the Data Subject as soon as practically possible. The Company must also notify the government authorities in accordance with the PDPA. Further, the Company shall provide a remedy to the Data Subject once it has been proved that the Company is at fault.

The Company reserves the right not to provide a remedy for the damage caused by the Data Subject's fault, cases of voluntarily disclosure of Personal Data to others and/or cases of ignoring security protection measures and procedures.

9. Storage Duration of Personal Data

The Company shall retain Personal Data only as long as it is necessary in accordance with the purposes and necessity of collection and possession of the Personal Data. The period of Personal Data possession shall be in accordance with the requirements of the applicable law for each matter. The Company shall retain Personal Data for a period of time after a contract has expired, provided that the said period is in accordance with prescription period as defined by relevant laws. The Company shall provide appropriate storage and/or systems to store each type of Personal Data. Under particular circumstances, such as pending litigation etc., the Company may have to retain Personal Data exceeding the prescription period. The ROPA specifies the period for which Personal Data must be retained.

If the Company stores Personal Data in a foreign country, the Company shall ensure that the data controller/data processor at the destination securely protects the Personal Data. The standard of data protection must be equally safe or better than that in this Policy.

In addition, the Company shall also require that employees, personnel, agents and third parties (including Data Processors) who receive Personal Data from the Company keep Personal Data confidential and secure as per the Company's measures when any processing of Personal Data is required.

10. Destruction of Personal Data

10.1 The Company must ensure that Personal Data is not kept beyond the retention period as specified in Article 9 above. The Company shall erase or destroy Personal Data after the expiration of the retention period specified for each type of data, when the Personal Data is no longer necessary for the purposes of the Company or the relevant law for collection, use or disclosure of such data, or upon a request from the Data Subject.

10.2 It is the responsibility of the relevant departments within the Company to examine and separate Personal Data that has reached the end of its retention period, as well as to destroy documents using the following means and methods:

10.2.1 If the Personal Data is stored in hard copy, destruction of the corresponding documents should be carried out by use of paper shredder.

10.2.2 If the Personal Data is stored in electronic files, the department which controls such documents should contact the IT Department to destroy the corresponding electronic files.

11. Rights of Data Subject

A Data Subject is entitled to request any actions regarding his/her Personal Data as follows:

11.1 Right to Withdraw Consent
Unless there is a restriction on the withdrawal of consent by laws, contractual obligations and/or other legitimate grounds, a Data Subject may withdraw his/her consent at any time. Withdrawing consent should be as simple as giving consent.

11.2 Right of Access
A Data Subject is entitled to request access to and obtain a copy of the Personal Data related to him/her, which is under the responsibility of the Data Controller, or to request disclosure of Personal Data obtained without his/her consent.

11.3 Right to Rectification
A Data Subject shall have the right to ensure that the Personal Data remains accurate, up-to-date, complete, and not misleading.

11.4 Right to Erasure
When the Personal Data is no longer necessary in relation to the purposes for which it was collected, used, or disclosed, or when the Data Subject withdraws consent on which the collection, use, or disclosure was based, and where the Data Controller has no legal grounds for such collection, use, or disclosure, the Data Subject shall have the right to request the Data Controller to erase or destroy the Personal Data, or anonymize the Personal Data such that it cannot identify the Data Subject.

11.5 Right to Restriction of Processing
A Data Subject shall have the right to request the Data Controller to restrict the use of the Personal Data in the following circumstances:
- When the Data Controller is in the process of verifying and/or examining the Data Subject's request; or
- When it is no longer necessary to retain such Personal Data for the purposes of such collection, but the Data Subject needs to request the retention for the purposes of establishment, compliance, exercise or defense of legal claims.

11.6 Right to Data Portability
A Data Subject shall have the right to receive the Personal Data concerning him/her from the Data Controller. The Data Controller shall arrange such Personal Data to be stored in a format that is readable or commonly used by way of automatic tools or equipment and can be used or disclosed by automated means. The Data Subject is also entitled to request the Data Controller to send or transfer the Personal Data in such formats to other Data Controllers if it can be done by automatic means or to directly obtain the Personal Data in such formats that the Data Controller sends or transfers to other Data Controllers unless it is impossible to do so because of technical reasons.

11.7 Right to Object
A Data Subject has the right to object to the collection, use, or disclosure of his/her Personal Data at any time.

A Data Subject may exercise any of these rights by sending a request in an **Electronic Form** or submit **Data Subject Action Request Form** along with all required documents to the Data Protection Officer (contact details as specified in Article 15 herein).

When the Company receives a request from a Data Subject, the Company shall consider the proper method to deal with such request within 30 days of the date of receipt thereof. The Company reserves the right to reject any request if the Company has legitimate grounds or is compelled by applicable laws to do so.

12. Enforcement

12.1 This Policy is applicable to the Board of Directors, Managing Director, Executives and all staff members at all levels.
12.2 This Policy is applicable to all of the Company's activities concerning Personal Data in any form.
12.3 All Departments in the Company involved with Personal Data must use any Personal Data with utmost caution and must strictly follow the guidelines in this Policy when collection, using and/or disclosing Personal Data.
12.4 Personal Data is kept strictly confidential. Accessing or misusing Personal Data without permission is considered as violation of the Company's Code of Conduct, the Company regulations and/or relevant laws. Disciplinary actions may be taken against a violator irrespective of whether any damage has occurred to the Data Subject.

13. Personal Data Breach

13.1 If any person finds any leakage of Personal Data or if there are reasonable grounds to suspect that there may be leakages of Personal Data or operations in connection with the collection, use or disclosure of Personal Data by the Company that are contradictory to or do not comply with the requirements of the PDPA and/or any related regulations and/or requirements under this Policy, please notify the Company's DPO via the channels specified in Article 15 of this Policy.
13.2 In accordance with the PDPA and any related regulations, the DPO and the company's senior management shall assess any breach of personal data and take any necessary actions.
13.3 Risks associated with personal data must be considered in the risk management of the organization and related agencies of the company, along with appropriate risk management and audit of operations related to personal data by the internal audit unit.
13.4 In accordance with the PDPA, the Company must notify the relevant government authorities of any leakage of personal data.

14. Review of Policy

The Company may review this policy from time to time to ensure that it is in accordance with applicable laws, the current situation, and/or any significant business changes.

15. Data Protection Officer

The Company has appointed the Data Projection Officer ("DPO") to advise on and monitor the conduct of the Company in compliance with the PDPA and relevant internal and guidelines on Personal Data protection. The DPO's roles and responsibilities must be in accordance with the PDPA.

Data Protection Officer

Name	Mr. Surasak Osathanugraha
Address:	Christiani & Nielsen (Thai) Public Company Limited No. 727 La Salle Road, Bangna-Tai, Bangna District, Bangkok 10260 Thailand
Telephone no.	+ 66 2 338 8000
Facsimile:	+ 66 2 338 8090
E-mail	surasakos@cn-thai.co.th

16. Contact Information

Data Controller

Company Name:	Christiani & Nielsen (Thai) Public Company Limited
Address:	No. 727 La Salle Road, Bangna-Tai, Bangna District, Bangkok 10260 Thailand
Tel:	+66 2 338 8000
Fax:	+66 2 338 8090
Email	cnt@cn-thai.co.th
Website	www.cn-thai.co.th

Government Authority

A Data Subject who wishes to contact the Government Authority that monitors and supervises the protection of Personal Data, may contact:

Authority:	Office of the Personal Data Protection Commission
Address	120, Village no. 3, Ratprasasanapukdee Building (Building B) The Government Complex Personal Data Protection Commission Ministry of Digital Economy and Society Chaengwattana Road, Thung Song Hong Sub-District, Laksi District, Bangkok 10210
Telephone no.	+ 66 2 142 1033
E-mail	pdpc@mdes.go.th

This Policy is announced on and is effective from 1 March 2022.