CORPORATE DATA PRIVACY POLICY

[Toshiba Tec (Thailand) Co., Ltd.]
(1 FEB 2022)

INTRODUCTION

[Toshiba Tec (Thailand) Co., Ltd.] (the **Company**) is bound by the provision of Personal Data Protection Act B.E. 2562 of Thailand (**PDPA**). The PDPA sets out standards, rights and obligations for how we handle and maintain people's personal data. This includes how we collect, store, use, disclose and secure the Data Subject's personal data, as well as Data Subject's acknowledging rights to their personal data.

The Company recognizes the importance of having an effective privacy protection measure in place and is committed to fully complying with the PDPA and all other laws related to data privacy to which it is subject. These protections are an integral part in ensuring we maintain our reputation as a trustworthy business operator, are necessary to maintain the confidence of our customers, business partners, and employees and to ensure the Company's own compliance with the PDPA. This Corporate Data Privacy Policy (the **Policy**) is based on the basic principle of the protection of data privacy under the PDPA.

The Policy outlines strict requirements for processing personal data pertaining to customers, prospects, business partners and employees. This Policy sets a locally applicable data protection and security standards for the Company and regulates the sharing of information between companies within our group of companies.

The Company's management and employees are to strictly adhere to the Policy and observe the related rules under the PDPA.

Date: 1 FEB 2022

PAUL TING
Chief Executive Officer

CORPORATE DATA PRIVACY POLICY

1. OBJECTIVE

The purpose of this Policy is to set out the rules, procedures and guidelines for the Company's personnel to ensure the privacy of personal data of candidates, employees, contractors, vendors, interns, associates, prospective customers, customers and business partners (the **Data Subjects**) of the Company and ensure compliance with PDPA.

2. SCOPE

This Policy is applicable to all the Company's personnel including but not limited to directors, full time and/or part time employees (**Company's Personnel**) who may receive and/or process personal data and/or have access to personal data collected or processed regardless of geographic location.

All Company's Personnel must strictly comply with this Policy when they collect and / or handle personal data or are involved in the process of maintaining or disposing of personal data. For avoidance of doubt, Anonymized data, e.g. for statistical evaluation or studies, is not subject to this Policy.

The Company's contractual counterparties and any third-party working with or for the Company, who have or may have access to personal data, will be expected to read, understand and fully comply with the Policy. No third party may access personal data held by the Company without having first entered into a non-disclosure agreement, a confidentiality agreement, or other similar instrument.

3. RESPONSIBILITIES

The responsible person for the Policy shall be the Data Privacy Officer (**DPO**). The DPO will work to ensure compliance with the PDPA. The DPO shall be appointed by the Company.

The DPO shall be responsible for:

(a) Personal Data maintenance and accuracy of this Policy and supervises its compliance.

(b) Any queries regarding the implementation of this Policy shall be directed to the DPO.

4. POLICY COMPLIANCE

In cases where non-compliance is identified, the DPO shall review the reasons for such non-compliance along with a plan for remediation and report them to the Chief Executive Officer (**CEO**) of the Company.

5. CHOICE AND CONSENT

Choice refers to the options the Data Subjects are offered regarding the collection and use of their personal data (**Choices**). Consent refers to agreements to the collection and use, often expressed by the way in which they exercise a choice option.

- The Company shall establish systems for the collection and documentation of Data Subjects' consents to the collection, processing, and/or transfer of personal data. The Choices shall be updated in a timely manner in accordance to the purposes/use of the personal data collected.

- Data Subjects shall be informed about the choices available to them with respect to the collection, use, and disclosure of personal data.

- Consent shall be obtained (in writing or electronically) from the Data Subjects before or at the time of collecting personal data or as soon as practical thereafter.

- The changes to Data Subjects' preferences shall be managed and documented. Consent or withdrawal of consent shall be documented appropriately.

- If personal data is to be used for purposes not identified in the notice / contract / agreements at the time of collection, the new purposes shall be documented, the Data Subjects shall be notified, and consent shall be obtained prior to such new use or purpose.

- The DPO shall review the privacy policies of the third parties and types of consent of third parties before accepting personal data from third-party data sources.

6. RELIABILITY OF DATA PROCESSING

Collecting, processing and using personal data is permitted only under the following legal bases. One of these legal bases is also required if the purpose of collecting, processing and using the personal data is to be changed from the original purpose.

6.1 Customers and Business Partner Data

6.1.1 Data Processing for a contractual relationship

- Personal data of the relevant prospects, customers and business partners can be processed in order to establish, execute, perform and terminate a contract. This also includes advisory services for the business partner under the contract if this is related to the contractual purpose.

- Pre-contractual phase – personal data can be processed to prepare bids or purchase orders or to fulfill other requests of the prospect that relate to contract conclusion.

- Prospects can be contacted during the contract preparation process using the information that they have provided.

6.1.2 Data Processing for the Company's own benefit

- Personal data can be processed for advertising purposes or market and opinion research, if that is consistent with the purpose for which the data was originally collected.

- When the sole purpose of obtaining data from Customer is for advertising/marketing or opinion research, the Customer must be made known of such purpose clearly and consent must be obtained prior to collection and/or process of such personal data. Consent obtained from Customer would signify that Customer voluntarily disclosed all data and agreed to their personal data being processed and/or use for such purposes. When obtaining consent, the customers shall be given a choice among available forms of contact such as regular mail, e-mail and phone.

- If customers refuse/ withdraw consent for the use of their personal data for advertising purpose, the Company must immediately cease using their personal data for such purpose.

6.1.3 Data Processing Pursuant to legal authorization

- The processing of personal data is also permitted if the law of Thailand requires or allows it. In such case, the type and extent of data processing must be necessary for the legally authorized data processing activity.

6.1.4 Data processing pursuant to legitimate interest

- Personal data can also be processed if it is necessary for a legitimate interest of the Company. Legitimate interests are generally of a legal (e.g. collection of outstanding receivables) or commercial nature (e.g. avoiding breaches of contract).

- Personal data may not be processed for the purpose of legitimate interest if, in individual cases, there is evidence that the interests of the customers or business partners merit protection, and that it takes precedence over the Company's legitimate interest.

- Before data is processed, it is necessary to determine whether there are interests that merit such protection.

6.1.5 Processing of Sensitive Personal Data

- Sensitive Personal Data can be processed only if the law requires, or the customers or business partners have given their express consent. Sensitive Personal Data includes data about racial and ethnic origin, political beliefs, religious or philosophical beliefs, union membership, disabilities, health and sexual life, criminal record, biometric data, and other similar data, of the data subject.
- Sensitive Personal Data can also be processed if it is mandatory for asserting, exercising or defending legal claims regarding the customers or business partners.

6.1.6 Automated individual decisions

- Automated processing of personal data that is used to evaluate certain aspects (e.g. credit worthiness) cannot be the sole basis for decisions that have negative legal consequences or could significantly impair the customers or business partners.

- The customers or business partners must be informed of the facts and results of automated individual decisions and the possibility to respond.

6.1.7 User data and the internet

- If personal data is collected, processed and used on websites or in apps, the data subjects must be informed of this in a privacy policy and, if applicable, information about cookies.

- If user profiles (tracking) are created to evaluate the use of web sites and apps, the data subjects must always be informed accordingly in the privacy policy.

- Personal tracking may only be effected if it is permitted under PDPA or upon consent of the customers or business partners.

- If websites or apps can access personal data in an area restricted to registered users, the identification and authentication of the customers or business partners must offer sufficient protection during access.

6.2 Employee Data

6.2.1 Data processing for the employment relationship

- In employment relationships, personal data can be processed if needed to initiate, carry out and terminate the employment agreement.

- When initiating an employment relationship, the candidates' personal data can be processed. If the candidate is rejected, his/her data must be deleted in observance of the required retention period, unless the applicant has agreed to remain on file for a future selection process.

- Consent is also needed to use the data for further application processes or before sharing the application with other entities in the group companies.

- In the existing employment relationship, data processing must always relate to the purpose of the employment agreement.

- Should it be necessary during the application procedure to collect information on a candidate from a third party, the requirements under the PDPA must be observed. In cases of doubt, consent must be obtained from the candidates.

- There must be legal authorization to process personal data that is related to the employment relationship but was not originally part of performance of the employment agreement. This can include legal requirements, collective regulations with employee representatives, consent of the employee, or the legitimate interest of the Company.

6.2.2 Data processing pursuant to legal authorization

- The processing of personal employee data is also permitted if the laws of Thailand requests, requires or authorizes such processing.

- The type and extent of data processing must be necessary for the legally authorized data processing activity and must comply with the relevant statutory provisions.

6.2.3 Data processing pursuant to legitimate interest

- Personal data can also be processed if it is necessary to enforce a legitimate interest of the Company. Legitimate interests are generally of a legal (e.g. filing, enforcing or defending against legal claims) or financial (e.g. valuation of companies) nature.

- Personal data may not be processed based on a legitimate interest if, in individual cases, there is evidence that the interests of the employee merit protection. Before data is processed, it must be determined whether there are interests that merit protection.

- Control measures that require processing of employee data can be taken only if there is a legal obligation to do so or there is a legitimate reason.

- Even if there is a legitimate reason, the proportionality of the control measure must also be examined. The justified interests of the Company in performing the control measure (e.g. compliance with legal provisions and the Company's internal rules) must be weighed against any interests meriting protection that the employee affected by the measure may have in its exclusion, and cannot be performed unless appropriate.

6.2.4 Processing of Sensitive Personal Data

- Sensitive Personal Data can be processed only under certain conditions.

- The processing must be expressly permitted or prescribed under the PDPA. Additionally, processing can be permitted if it is necessary for the responsible authority to fulfill its rights and duties in the area of employment law. The employee can also expressly consent to processing.

6.2.5 Automated decisions

- If personal data is processed automatically as part of the employment relationship, and specific personal details are evaluated, this automated processing cannot be the sole basis for decisions that would have negative consequences for the affected employee.

- To avoid erroneous decisions, the automated process must ensure that a natural person evaluates the content, and that this evaluation is the basis for the decision. The employees must also be informed of the facts and results of automated individual decisions and the possibility to respond.

6.2.6 Telecommunications and internet

- Telephone equipment, e-mail addresses, intranet and internet along with internal social networks are provided by the Company primarily for work-related assignments. They are a tool of and the Company's resource. They can be used only within the applicable legal regulations and the internal Company policies.

- For security reasons, the use of telephone equipment, e-mail addresses, the intranet and internal social networks can be logged for a temporary period.

7. PRIVACY POLICY

A privacy policy shall be made readily accessible and available to Data Subjects on or before or at the time of collection or personal data or otherwise, it shall be provided as soon as practical thereafter. The privacy policy shall be displayed clearly and conspicuously and shall be provided through [online (e.g. posting it on the intranet portal, website, sending mails, newsletters, etc.) and / or offline methods (e.g. through posts, couriers, etc.)][1] All web sites (including Intranet portals), and any product or service that collects personal data internally, shall have a privacy policy.

In case of any cross-border transfer of personal data, the Data Subjects shall be informed by a notice sufficiently prior to the transfer unless covered by the privacy policy.

In the event of such situations not covered under the privacy policy, the notices may include:

- The Company's operating jurisdictions; third parties involved; business segments and affiliates; lines of business; locations;

[1] Company to check how the Notice will be circulated to the data subjects.

- types of personal data collected; sources of information; who is collecting the personal data, including contact information;
- the purpose of collecting the personal data;
- assurance that the personal data will be used only for the purpose identified in the notice and only if the implicit and / or explicit consent is provided unless a law or regulation specifically requires otherwise;
- any choices the Data Subjects have regarding the use or disclosure of the information; the process and Data Subjects shall follow to exercise the choices;
- the process for Data Subjects to change contact preferences and ways in which the consent is obtained.
- collection process and how the information is collected; how the information is used including any onward transfer to third parties;
- retention and disposal process for personal data; assurance that the personal data to be retained only as long as necessary to fulfill the stated purposes, or for a period specifically required by law or regulation and will be disposed of securely or made anonymous once the identified purpose is completed;
- security measures in place to protect the personal data; ways of maintaining quality of personal data;
- monitoring and enforcement mechanisms in place; description of the complaint channels available to Data Subjects; how the internal personnel, key stakeholders and the customers can contact the Company related to any privacy complaints or breaches; relevant contact information and / or other reporting methods through which the complaints and/or breaches could be registered; and
- consequences of not providing the requested information.

8. COLLECTION OF PERSONAL DATA

Personal data may be collected online or offline. Regardless of the collection method, the same privacy protection shall apply to all personal data.

- Personal data shall not be collected unless any of the following are fulfilled below:
    - the Data Subject has provided a valid, informed and free consent;
    - processing is necessary for the performance of a contract to which the data subject is a party or in order to take steps at the request of the Data Subjects prior to entering into a contract;
    - processing is within legitimate interest of the Company;
    - processing is necessary for compliance with the Company's legal obligation;
    - processing is necessary in order to protect the vital interests of the Data Subjects; or
    - processing is necessary for the performance of a task carried out in the public interest.

- Data Subjects shall not be required to provide more personal data than is necessary for the provision of the products or services that Data Subjects have requested or authorized. If any data not needed for providing services or products are requested, such fields shall be clearly labeled as optional. Collection of personal data shall be avoided or limited when reasonably possible.

- When using vendors to collect personal data on the behalf of the Company, it shall ensure that the vendors comply with the privacy requirements of the Company as defined in this Policy.

- The Company shall review the Policy and collection methods of third parties before accepting personal data form third-party data sources.

9. USE, RETENTION AND DISPOSAL

- Personal data may only be used for the purposes identified in the notice / contract agreements and only if the Data Subjects have given consent.

- Personal data shall be retained for as long as necessary for business purposes identified in the notice / contract agreements at the time of collection or subsequently authorized by the Data Subjects.

- When the use of personal data is no longer necessary for business purposes, a method shall be in place to ensure that the information is destroyed in a manner sufficient to prevent unauthorized access to that information or is de-identified in a manner sufficient to make the data non-personally identifiable.

- The Company shall have a documented process to communicate changes in retention periods of personal data required by the business to the Data Subjects who are authorized to request those changes.

- Personal data shall be erased if its storage violates any of the data protection rules or if knowledge of the data is no longer required by the Company or for the benefit of the Data Subjects. Additionally, the Company has the right to retain the personal data for legal and regulatory purpose and as per the PDPA and other applicable laws.

10. ACCESS

The Company shall establish a mechanism to enable and facilitate exercise of Data Subjects' rights of access, blockage, erasure, opposition, rectification, and, where appropriate or required by applicable law, a system for giving notice of inappropriate exposure of personal data.

- Data Subjects shall be entitled to obtain the details about their own personal data upon a request made in writing.

- The Data Subjects shall have the right to require the Company to correct or supplement erroneous, misleading, outdated, or incomplete personal data.

- The Company shall record and document each access request it receives, and the corresponding action taken with respect thereto.

- The Company shall provide personal data to the Data Subjects in a plain simple format which is understandable (not in any code format).

11. DISCLOSURE TO THIRD PARTIES

Data Subjects shall be informed in the privacy notice / agreement, if personal data shall be disclosed to third parties / partner firms, and it shall be disclosed only for the purposes described in the privacy notice / agreements and for which the Data Subjects have provided consent.

- Personal data of Data Subjects may be disclosed to the third parties / partner firms only for reasons consistent with the purpose identified in the notice / agreements or other purposed authorized by the PDPA and other applicable laws.
- The Company shall notify the Data Subjects prior to disclosing personal data to third parties / partner firms for purposes not previously identified in the notice / agreements.
- The Company shall communicate the privacy practices, procedures and the requirements for data privacy and protection to the third parties / partner firms.
- The third parties shall sign a Non-Disclosure Agreement (**NDA**) with the Company before any personal data is disclosed to the third parties partner firms. The NDA shall include the terms on non-disclosure of customer information.

12. TRANSMISSION OF PERSONAL DATA

- Transmission of personal data to recipients outside or inside the Company is subject to the authorization requirements for processing personal data. The data recipient must be required to use the date only for the defined purposes.

13. SECURITY

Information security policy and procedures shall be documented and implemented to ensure reasonable security for personal data collected, stored, used, transferred and disposed by the Company.

- Information asset labeling and handling guidelines shall include controls specific to the storage, retention and transfer of personal data.
- Incident response protocols are established and maintained in order to deal with incidents concerning personal data or privacy practices.

14. QUALITY

The Company shall maintain data integrity and quality, as appropriate for the intended purpose of personal data collection and use and ensure data is reliable, accurate, complete and current.

- For this purpose, DPO shall have systems and procedures in place to ensure that personal data collected is accurate and complete for the business purposes for which it is to be used.

This Policy is established and effective on 1 FEB 2022 **. If the related clauses of the PDPA or other related laws are amended, the provisions of the law shall automatically prevail.**