

# Privacy Policy for Employees and Job applicants

## Tokio Marine Safety Insurance (Thailand) PCL.

### Purpose

Tokio Marine Safety Insurance (Thailand) PCL. (“the company”) realized the importance of privacy rights and it is the company’s responsibility to safely collect, use and disclose (collectively as “Processing personal data”) personal data for employees and job applicants. The objective of this policy is to inform regarding how the company process personal data of employees and job applicants in accordance with the Personal Data Protection Act B.E. 2562 (“PDPA”).

### Definition

“Personal Data”	means	Any information relating to a person, which enables the identification of such person, whether directly or indirectly, but not including the information of the deceased persons in particular and not including juristic person information.
“Sensitive Data”	means	Information which stated in Section 26 of Personal Data Protection Act and the amendments and other relating laws and regulations including information regarding racial, ethnic origin, political views, religious or philosophical beliefs, sexual behavior, criminal records, health data, disability, trade union information, genetic data, biometric data, or other data which may affect the data subject in the same manner.
“ Personal Data Protection Act – PDPA”	means	Personal Data Protection Act B. E. 2562 including subordinate laws which published under Personal Data Protection Act and its amendments.
“Committee”	means	the Personal Data Protection Committee

# 1. Collecting of Personal Data

## 1.1 For Job applicants

- 1) Any identification information of such person, for example, name, address or other contact address, gender, age, nationality, marital status, date of birth, house registration, driving license, passport number, ID card number, person who is in the care of job applicant and photo.
- 2) Qualification and working experience, for example, certificate from school/university, learning history, academic or language test, professional license (such as agent/broker license) other certificate and reference.
- 3) Sensitive data, for example, health data, criminal record which the company will collect such sensitive data when job applicant pass the job interview. It is necessary for the company to collect sensitive data for employment contract process and assessment readiness for work.
- 4) Personal data of related person, for example, reference person and contact person.

## 1.2 For Employees

When job applicant pass the interview and sign the employment contract, the company will collect and process personal data which were collected during recruitment process and will collect additional personal data as follows:

- 1) Employment details, for example, employee ID, job position, chain of command, working time, employment rule and condition.
- 2) General work performance, for example, personal profile, military status, job interview, job interview assessment form and reference, in-out of workplace record, CCTV, phone record, email, internet usage data regarding work performance which is not illegal.
- 3) Benefit and compensation, for example, bank account, details of salary and other benefits, social security, retirement/pension information, provident fund, tax and other third-party beneficiary information.
- 4) Work efficiency including assessment, response, rule and regulation for work or complaint annual leave record, sick leave record or absence record, workplace and security in workplace including audit and risk assessment.
- 5) Sensitive data, for example, health record for providing welfare and benefit such as health insurance or reimbursement of medical expenses.

In case that employee provide personal data of other person to the company, for example, family member or relative for emergency situation or employee benefit management. Employee acknowledge and confirm that they inform this policy to such person. In case that the company need

to receive their consent, employee must proceed in order to the company can process their personal data of such person legally.

## 2. Personal Data Management

Personal data collection of employee and job applicant. In general, the company collect personal data directly from employee and job applicant. In some case, the company may collect such personal data from other source or third party, for example, recommendation person, recruitment agency, hospital, government agency.

## 3. Purpose of Processing Personal Data

### 3.1 For job applicants

For recruitment process, such as profile consideration, interview, document preparation, health check management and other related conduct.

### 3.2 For employees

- 1) For considering employment condition, employment contract preparation including signing such contract.
- 2) For performing right and duty in accordance with employment contract between employee and the company.
- 3) For management regarding working, welfare of employee or third party (if any) in accordance with employment contract including assessment, training and human resource management such as background checks in accordance with laws, physical information, providing assistance to employee for adjusting to new job, welfare management, employee information record, insurance application, medical record and insurance plan, recruitment and training management, promotion, transfer, assignment and for compliance with laws and regulations including manpower planning, wages, compensation, benefit, remuneration planning, future proposal, reward, account, remuneration, work performance assessment, internal report, data analysis and monthly/daily employment management, internal communication, making appointment both internal and external, consideration of job application form for new opportunity and making decision for employment including promotion assessment, work performance, and assessing equality of opportunity.
- 4) For research, data analysis and making statistics in the field of employment, assessment or other related employment and human resource management process including making survey, government statistics or answering government request form.
- 5) For proceeding in accordance with the company's internal policy.
- 6) For personal data management including collect, record, spare or dispose of personal data.

- 7) For monitoring employee behavior which includes validation and investigation of complaint regarding inappropriate behavior, violation of the company rules and/or laws either for internal investigation or cooperation with government agency.
- 8) For analysis and training to improve potential and ability of work performance.
- 9) For compliance with laws and business audit both internal audit and external audit.
- 10) For proceeding in accordance with laws, regulations or policies which stipulated by governing regulators, governmental law enforcement, governmental dispute resolution or insurance regulator and other related agency.
- 11) For law enforcement purpose or assisting, cooperating, investigating by the company or police officer or government agency or other domestic regulator, reporting according to the regulations or as agree with government agency or regulators domestically or as ordered by the government officers or government agency.
- 12) For security of employee or others who entering and leaving the office building.
- 13) For the company restructuring and the company transaction.
- 14) For purchasing or selling one or more than one business (part of business) of the company.
- 15) For proceeding others if necessary which relating to the above purposes unless stipulated by laws and regulations including PDPA. The company will obtain consent prior to processing personal data for the purposes other than specify in this policy or relating to the purposes under this policy.

## 4. Disclosing of Personal Data

In order to carry out the above purposes, the company may have to disclose employee or job applicant's personal data to third party as stated below.

- 1) Group companies.
- 2) The company's adviser, expert or Group Company's adviser such as lawyer, auditor or consultant.
- 3) Third-party service provider or service provider agent who need to perform according to above purposes such as agent/broker, insurance company, recruitment agency, support service provider for information technology system or recruitment system, accounting system, payroll system and other human resource information system.
- 4) Law enforcement regulator, commission which established by law, government sector or regulators, governmental dispute resolution or other party which the company or group company require to disclose information (a) according to the laws or regulations in Thailand and may include government sectors which the group company located or (b) according to agreement or corporate rules between the company and government sectors or other relating parties.

- 5) A person or entity who enter into or will enter into any transaction with the company which employee or job applicant's personal data may be part of purchasing or selling or offering to purchase or sale the company's business. (If any)
- 6) Personnel or sector which employee or job applicant explicitly consent the company to disclose personal data to.
- 7) Provident fund in order to achieve above purposes.

## 5. Disclosing Personal Data Outside of Thailand

Employees or Job applicants's personal data may be disclosed, stored or processed by the company or transferred to external parties which may be located or provide service inside or outside of Thailand. However, personal data will be transferred in accordance with Personal Data Protection Act. If the transfer is between group companies, the company will proceed in accordance with the Binding Corporate Rules which has been approved by Personal Data Protection Commission.

## 6. Retention of Personal Data

The company will retain personal data as necessary for proceeding in accordance with above purposes.

- 6.1 For Job applicant who is not selected. Personal data will be retained for 2 years since the date of receipt from job applicant unless stipulated by laws.
- 6.2 For Employee who enter into service agreement with the company. Personal Data will be retained during employment and for 10 years since the date of valid resignation unless stipulated by laws.

## 7. Rights of Data Subject

Employees or Job applicants may exercise the rights regarding personal data as following:

- 1) Withdraw or request to change the scope of consent which have given to the company.
- 2) Verify personal data which stored with the company including request to access or copy personal data and/or access to the data to know how the company process personal data.
- 3) Correct personal data.
- 4) Delete or dispose personal data.
- 5) Restrict the processing of personal data.
- 6) Transfer personal data.
- 7) Temporary restrain processing of personal data.

The company reserve the right to not following the request under the company discretion and in accordance with the laws. Employee and Job applicant may file a complaint to The Personal Data Protection Committee (PDPC) as procedures provided in the Personal Data Protection Act (PDPA).

The company may not follow the request if such request affect the processing of personal data for above purposes including status of employee or job applicant and in accordance with the laws. The company may collect fees for processing the request as the company see suitable.

## 8. Revision to this Policy

The company reserve the rights to amend, revise, or made any change to this policy as allow by laws. If there is a significant amendment to this policy, the company shall inform employees or job applicants for such amendment and/or obtain consent from employees or job applicants (if stipulated by laws).

## 9. Contact Information

If employees or job applicants have any inquiries related to this policy or need more information or would like to exercise data protection rights. Please contact at:

**Data Protection Officer (DPO)**

**Tokio Marine Safety Insurance (Thailand) PCL.**

Address: No. 302 S & A Building, 6<sup>th</sup> Floor, Silom Road, Suriyawong, Bangrak, Bangkok 10500

Tel. 02-257-8000 at 8.30 - 16.45

Email: [DPO@tokiomarinesafety.co.th](mailto:DPO@tokiomarinesafety.co.th)