

## Privacy Policy (Singapore Branch)

### ○ Section 1 Handling of Personal Information

1. The Toa Reinsurance Company Limited (Singapore Branch) (the “Company”) is committed to the protection of personal data in compliance with the Personal Data Protection Act 2012 of Singapore (“PDPA”). However, as a matter of policy, the Company has no need to and does not actively or passively collect, use or disclose the personal data of individuals in the course of conducting its re-insurance business.
2. All clients of the Company are and shall be required to ensure that unless otherwise expressly agreed with or required by the Company, any and all documentation and/or information (including data concerning any existing insurance policies, or proposals or benefits) provided to the Company pursuant to or for the purpose of any reinsurance contract (including to facilitate the Company in assessing/evaluating any claim) shall not contain the personal data of any individual (as understood within the context of the PDPA). Alternatively, the client shall ensure that all documentation or information submitted to the Company shall be anonymised or pseudonymised so that no individual can be identified.
3. In the event that any documentation received by the Company from its clients should inadvertently contain any personal data, the Company shall be deemed to receive such personal data solely in the capacity of a data intermediary (as understood within the context of the PDPA) and the Company shall, acting in such capacity, have the authority and power to redact such personal data from the documentation on behalf of the client.

## ○ Section 2 Handling of Specific Personal Information

The Toa Reinsurance Company Limited (Singapore Branch)(the “Company”) is committed to the protection of personal data in compliance with the Personal Data Protection Act 2012 of Singapore (“PDPA”). This includes the personal data of all job applicants, present employees, and former employees of the Company (collectively, the “Employees”, and each of the Employees being an “Employee”).

This Policy for the Protection of Personal Data of Employees (“Policy”) contains the details of how the Company will collect, use, disclose and otherwise manage the Employees’ personal data, and applies to all Employees whose personal data is in our possession or under our control. The Company may amend this Policy from time to time by posting an amended version of this Policy on the Company’s website.

Please note that this Policy only serves to provide you with an overview of the obligations that the Company will comply with in respect of the Employees’ personal data pursuant to the PDPA. The Employees are advised to refer to the PDPA or the Personal Data Protection Commission website (<http://www.pdpc.gov.sg> ) for full details of the PDPA.

### **1.Acquisition, Use and Disclosure of Personal Data**

The Company collects or has collected personal data of Employees from time to time through the Employees’ curriculum vitae, employment history, and other documentation provided by such said Employees, employment agencies or portals, and/or other sources, and the Company will use and disclose any such personal data only in a lawful and proper manner.

### **2. Purposes of Collection, Use and Disclosure of Personal Data**

2.1 The Company may collect, use and/or disclose the personal data of Employees for one or more of the purposes described below:

- 2.1.1 To manage the employment relationship of each Employee with the Company (and the termination thereof), including but not limited to:
  - 2.1.1.1 Administration of pay and benefits;
  - 2.1.1.2 Audit of company records, including employee records;
  - 2.1.1.3 Application for employment pass/work permit/visa;
  - 2.1.1.4 Payment of CPF;
  - 2.1.1.5 Holding as part of the Company's records as to the business carried on by the Company;
  - 2.1.1.6 Filing of income tax details;
  - 2.1.1.7 Organisation of volunteer activities and charitable giving;
  - 2.1.1.8 Facilitation of communication within the Company and the Company's related companies through the use of global and local directories;
  - 2.1.1.9 Monitoring of each Employee's compliance with company policies, conduct of performance reviews and determination of performance requirements;
  - 2.1.1.10 Establishment of training and development requirements;
  - 2.1.1.11 Management of medical leave, evaluation of employee wellness programmes, health benefits and health insurance; and
  - 2.1.1.12 Investigation into complaints and disciplinary issues and conduct of disciplinary and grievance procedures, including keeping records thereof;
- 2.1.2 For evaluative purposes, namely, to determine each Employee's eligibility for employment, continued employment, or promotion;
- 2.1.3 To observe any legal, governmental or regulatory requirements of any relevant jurisdiction (including any disclosure or notification requirements to which the Company is subject);
- 2.1.4 To comply with the Company's policies and procedures and those policies and procedures of the Company's related companies (including without limitation any reporting and disclosure policies and procedures); and

2.1.5 To carry out due diligence, monitoring or other screening activities in accordance with the Company's legal or regulatory obligations or risk management procedures,

(collectively, the "Purposes"). The Company may modify or expand the Purposes only to the extent reasonably deemed to have significant relevance to any of the original Purposes. In such cases, the Company will officially announce the details of the modification or expansion on its website or by other means. The Company will not collect, use and/or disclose personal data for any other purpose, save where the relevant Employee has given consent for or is deemed to have consented to such collection, use and/or disclosure.

### **3. Provision of Personal Information to Third Parties**

3.1 The Company may disclose personal data of the Employees to the following parties (whether such parties are located or resident within or outside Singapore) for one or more of the Purposes:

3.1.1 any parties in the course of the mailing of correspondence or any other relevant document(s) to each Employee, which could involve disclosure of certain personal data about the Employee to bring about delivery of the same;

3.1.2 employees, officers, directors and agents of the Company;

3.1.3 the Company's related companies (to comply with the Company's policies and procedures and those policies and procedures of the Company's related companies);

3.1.4 the Company's lawyers and auditors;

3.1.5 any third party vendors employed or engaged to provide administrative, computer or other services or facilities to the Company;

3.1.6 any regulatory authority, government, dispute resolution or statutory body in Singapore and/or other jurisdiction/s; and

3.1.7 such further or other parties who have a “need to know” such personal data for the Purposes above as the Company may in good faith determine,

(collectively, the “Permitted Parties”).

3.2 The Company shall not provide personal data it has collected to any third party except in accordance with relevant laws or ordinances.

3.3 When outsourcing the handling of personal data to external institutions where necessary for achievement of the purposes of the Company’s collection, use, and/or disclosure of such personal data, the Company applies criteria for selection of institutions to which the handling is to be outsourced, checks in advance the personal information management systems of the institutions, and carries out necessary supervision of the institutions, including monitoring of the institutions’ performance of the relevant personal data handling services even after the Company has outsourced the handling of personal data.

#### **4. Consent and the Withdrawal of Consent**

4.1 Every Employee who voluntarily provides his/her personal data to the Company, whether directly or through a third party source such as an employment agency or portal or in response to the Company’s request or through the Employee’s job application, curriculum vitae, employment history, or any other document, is deemed to have been notified of the Purposes and to have consented to the collection, use and disclosure by the Company of such personal data for any of the Purposes.

4.2 Subject to paragraph 4.3, if the Company wishes to collect, use, and/or disclose an Employee's personal data for purposes other than the Purposes, the Company will inform the Employee of those purposes and obtain his/her consent through a consent form ("Form"), save in accordance with any laws. By signing on a Form, the Employee consents to:

4.2.1 the Company processing, collecting, using and/or disclosing his/her personal data for the purposes described therein;

4.2.2 the Company collecting personal data about the Employee from sources other than the Employee and using and/or disclosing such personal data, for the purposes described therein; and

4.2.3 the Company disclosing his/her personal data to the Permitted Parties, for the purposes described therein.

4.3 The Company may collect, use and/or disclose an Employee's personal data obtained from third parties for purposes other than the Purposes, where the Employee had voluntarily provided the personal data to such third parties and consented to or are deemed to have consented to the disclosure by such third parties to the Company for those purposes.

4.4 An Employee may withdraw his/her consent to the collection, use and/or disclosure of his/her personal data by the Company for any purpose by written notice to the Company's data protection officer(s), delivered by way of e-mail transmission, providing relevant details of the personal data and the purposes of collection, use and/or disclosure thereof for which the Employee is withdrawing his/her consent.

4.5 The Company may not be able to manage its employment relationship with its present employee if he/she withdraws his/her consent to the collection, use and/or disclosure of his/her personal data by the Company for any of the Purposes. The Company's data protection officer(s) will notify an Employee of the consequences of the withdrawal of his/her consent by way

of e-mail within reasonable period of time of receipt of the Employee's notice of withdrawal of his/her consent pursuant to paragraph 4.4. Should the Employee confirm his/her decision to withdraw his/her consent by way of e-mail in reply to such notice by the Company's data protection officer(s), the Employee will be deemed to have accepted the consequences of the withdrawal of his/her consent as set out in the notice, and the Company will thereafter cease (and cause the Company's data intermediaries and agents to cease) collecting, using and/or disclosing the personal data for such purposes as conveyed in the Employee's notice.

## **5. Accuracy**

Any personal data voluntarily provided by an Employee will be deemed to be accurate and complete. Where an Employee's personal data has been provided to the Company by a third party, the Company may request the Employee to verify the accuracy and completeness of his/her personal data from time to time.

## **6. Access and Correction of Personal Data in Accordance with the Personal Data Protection Act**

6.1 An Employee may request to have access to his/her personal data in the Company's possession or under its control, and information about the ways in which such personal data may have been used and/or disclosed by the Company within the period of one year before the date of request, by way of an e-mail to the Company's data protection officer(s) with sufficient detail to enable the Company, with a reasonable effort, to identify the Employee, and the requested personal data and use and disclosure information. The Company may charge a reasonable fee for services provided to respond to such a request. Subject to exceptions set out in any relevant laws, the Company will provide the Employee access to his/her personal data in its possession or under its control and information about the ways in which his/her personal data may have been disclosed and/or used.

6.2 An Employee may request to correct an error or omission in his/her personal data in the Company's possession or under its control by way of an e-mail to the Company's data protection officer(s) with sufficient detail to enable the Company, with a reasonable effort, to identify the Employee, the personal data in question and the requested correction. Subject to the exceptions set in any relevant laws, the Company will respond to such a request, or otherwise inform the Employee of such other time by which it will respond, within 30 days after its receipt.

## **7. Summary of Measures to Ensure the Secure Management of Personal Data**

The Company has established the Preventative Measures for Personal Data/Classified Information Leakage and other rules to prevent any divulgence or loss of or damage to personal data handled by the Company and to ensure that personal data is otherwise securely managed and has implemented security measures, including the establishment of a structure for enforcing security management measures based on those rules and regulations, including the following measures:

7.1.1 in respect of the Employee's personal data stored in electronic form, the Company has adopted the following technical measures:

7.1.1.1 ensuring that computer networks are secure;

7.1.1.2 adopting appropriate access controls (e.g. considering stronger authentication measures where appropriate);

7.1.1.3 encrypting personal data to prevent unauthorised access;

7.1.1.4 activating self-locking mechanisms where computers are left unattended for a certain period;

7.1.1.5 installing appropriate computer security software and using suitable computer security settings;

7.1.1.6 disposing of personal data in IT devices that are to be recycled, sold or disposed;

7.1.1.7 updating computer security and IT equipment regularly; and

7.1.1.8 ensuring that IT service providers are able to provide the requisite standard of IT security;

7.1.2 in respect of the Employee's personal data stored in physical form, the Company has adopted the following physical measures:

7.1.2.1 marking confidential documents clearly and prominently;

7.1.2.2 storing confidential documents in locked file cabinet systems;

7.1.2.3 restricting employee access to confidential documents on a need-to-know basis;

7.1.2.4 proper disposal of confidential documents that are no longer needed, through shredding or similar means;

7.1.2.5 implementing an intended mode of delivery or transmission of personal data that affords the appropriate level of security;

7.1.2.6 providing a summary of the personal data contained in storage so that personal data is accessed only when necessary; and

7.1.2.7 confirming that the intended recipient of personal data is the correct recipient to avoid undue disclosure of personal data;

7.1.3 in respect of the Employee's personal data, the Company has adopted the following administrative measures:

7.1.3.1 incorporating confidentiality obligations in the employment agreements of all employees;

7.1.3.2 conducting regular training sessions for staff to impart good practices in handling personal data and strengthen awareness of threats to security of personal data; and

7.1.3.3 ensuring that only the appropriate amount of personal data is held by the Company.

## **8. Retention and Cessation of Use of Personal Data**

8.1 Subject to paragraph 8.2, the Company will retain each Employee's personal data for as long as the Employee remains an employee of the Company and for seven years thereafter, or for any longer period as the Company may deem reasonable at its sole discretion.

8.2 The Company will ensure that it does not retain the Employees' personal data beyond the period during which:

8.2.1 one or more of the purposes for which such personal data was collected remains valid, or

8.2.2 retention of such personal data is necessary for legal or business purposes, including but not limited to where:

8.2.2.1 the personal data is required for an ongoing legal action involving the Company;

8.2.2.2 retention of the personal data is necessary in order to comply with the Company's obligations under other applicable laws, regulations, and international/regional/bilateral standards; or

8.2.2.3 the personal data is required for the Company to carry on its business operations, such as to generate annual reports or performance forecasts,

and ensure that the Company's agents and data intermediaries do not retain the Employees' personal data beyond this period.

8.3 At the end of the relevant period for the retention of the Employees' personal data by the Company described in paragraph 8.2, the Company will shred all physical copies and delete all electronic copies containing such personal data, or anonymise such personal data, as may be appropriate.

## **9. Transfer of Personal Data Overseas**

9.1 Where the Company transfers any of the Employees' personal data to a recipient in a country or territory outside Singapore, the Company will take appropriate steps to ascertain whether, and to ensure that, the recipient is legally bound to provide to the personal data a standard of protection that is at least comparable to the protection under the PDPA.

9.2 If the standard of protection provided by the recipient will not be similar to that provided by the Company pursuant to the relevant paragraphs of this Policy, the Company will either provide the relevant Employees a separate reasonable written summary of the extent to which their personal data will be protected by the recipient to a standard comparable to the protection under the PDPA so that the Employees may thereafter give their consent to the transfer of their personal data, or the Company will ensure the transfer is necessary for the entry into or performance of any employment contract between the Employees and the Company, or that any other exceptions set out in relevant laws apply to allow or require the Company to disclose the personal data to the recipient without the Employees' consent.

## 10. Data Protection Officer

10.1 The Company has designated the following individual(s) to be responsible for ensuring that the Company complies with the PDPA:

Name	Business Contact Information
Shiko Misono	E-mail address: <a href="mailto:Misono.S@sin.toare.co.jp">Misono.S@sin.toare.co.jp</a>
Nelly Yeo	E-mail address: <a href="mailto:Nelly.Y@sin.toare.co.jp">Nelly.Y@sin.toare.co.jp</a>

10.2 Any Employee who has any complaints in relation to the Company's collection, use, disclosure, or other dealings with his/her personal data may contact the Company's data protection officer(s), who will respond to the Employee's concerns on the Company's behalf, in conjunction with or under the supervision of relevant officers, employees, directors, and/or agents of the Company, where appropriate.