SOMPO

Global Data Protection Policy

1. Goals of this Data Protection Policy

Sompo International[1] is committed to **(1)** ensuring that its customers, counterparties, regulators, employees and shareholders have confidence in its ability to protect Data (as defined in this Policy) that it holds and uses in its business, **(2)** complying with all applicable data protection and privacy laws and regulations[2] and **(3)** respecting the privacy and data protection rights of all those from whom it may collect Data, as defined below, all as required by applicable law and regulations.

2. Application of this Policy

2.1 Worldwide Application. This Policy applies worldwide to all employees, operations and businesses of Sompo International that collect, use or process any Data, including all cross-border data transmissions and use of any Data by any affiliate of Sompo International or any third party vendor of Sompo International at any location anywhere in the world.

2.2 Global Standards. Sompo International subsidiaries may not adopt local policies, procedures or working guidelines affecting the use of any Data or the use of such Data that are inconsistent with or deviate from the requirements of this Policy without the prior approval of the Sompo International Chief Compliance Officer (the "Chief Compliance Officer").

2.3 Application to Vendors & Third Parties. All third party contractors, vendors and service providers of Sompo International shall comply with this Policy to the extent that any such contractor, vendor or service provider collects, uses or processes any Data for or on behalf of Sompo International. The Chief Compliance Officer shall ensure that appropriate measures are implemented to ensure such compliance, including appropriate guidelines required by this Policy or applicable laws and regulations that are incorporated into the contracts and other documentation that set forth the terms and conditions of the agreement with Sompo International.

---

[1] The term "Sompo International" refers to and includes all subsidiaries of Sompo International Holdings Ltd., a Bermuda exempted company ("SIH"). To the extent, however, that an affiliate of SIH that is not a subsidiary of SIH receives or uses data that is covered by this Global Data Protection Policy and requires protection under applicable law or regulation, then such affiliate is included within "Sompo International" for purposes of protecting the data that such affiliate receives or uses.

[2] The Chief Compliance Officer, with the assistance of the Legal & Compliance Department, shall maintain and update from time to time, as necessary, the applicable data protection and privacy laws and regulations from around the globe that apply to the business of Sompo International.

3. Impact of National or Local Laws

3.1 Chief Compliance Officer. The Chief Compliance Officer, with the assistance of the Legal & Compliance Department, shall (i) facilitate the compliance of each Sompo International subsidiary with this Policy and all applicable laws and regulations concerning the reporting of information about Data in the jurisdiction in which such subsidiary is located and (ii) resolve any issue concerning any conflict between the requirements of this Policy and the application of any applicable law or regulation.

3.2 Local Compliance or Privacy Officer. The Chief Compliance Officer shall organize and oversee a network of local compliance or privacy officers for the purpose of implementing this Policy throughout Sompo International. Each local compliance or privacy officer shall have responsibility for identifying operations and functions within the local compliance or privacy officer's territory and ensure that such operations and functions comply with this Policy.

3.3 Violations or Potential Violations. If at any time, any employee, client or third party vendor of a Sompo International subsidiary or affiliate believes that this Policy has been violated, an applicable law or regulation has been violated or that a requirement of this Policy contradicts or requires such employee, client, affiliate or vendor to violate any applicable law or regulation, then such employee, such client, such affiliate or such vendor, as the case may be, shall promptly notify the Chief Compliance Officer, the local compliance or privacy officer or another member of the Legal & Compliance Department. In such notice, such employee, client or vendor shall provide reasonable details describing such violation or potential violation.[3] The Chief Compliance Officer and Legal & Compliance department shall identify the violation or potential violation and ensure that appropriate mitigation measures for properly managing such violation or potential violation are implemented in accordance with this Policy and the applicable Sompo International risk management policy.

4. Data and Information Protected by this Policy

4.1 Definitions of Data and Personal Data. This Policy applies to all Data collected or obtained by Sompo International that is required to be protected by applicable law or regulations, regardless of whether such Data is held within Sompo International's systems or outside such systems with an affiliate, a third party vendor or at an employee's location outside a Sompo International office. For purposes of identifying information that must be protected, the following terms used in this Policy shall have the following meanings:

[3] As a supplement to this Section, Personal Data Breaches are addressed in Section 6.2 of this Policy.

(i) "**Data**" means all information Processed and recorded in any location, whether located within an office of Sompo International or elsewhere, by means of electronic equipment (e.g. computer systems, desk top computers, laptops and notebooks, mobile phones or smart phones, CCTV, embedded chips) or held in any structured manual filing system.

(ii) "**Data Processor**" means and includes any legal or natural person, wherever located, that Processes Data on behalf of Sompo International.

(iii) "**Data Subject**" means a living individual who is the subject of Personal Data. It includes employees, consultants, prospective and actual policyholders, clients, claimants and beneficiaries (to the extent named individuals) and individuals about whom business contact information may be held (for example, contacts at suppliers, advisors, etc.).

(iv) "**Personal Data**" means Data, directly or indirectly, relating to an identified or identifiable living individual, including Data that is available in the public domain, Data that may be fact or opinion and Data that may be personal, business or professional information. Data relating to a living individual, for example, includes an identifier such as a name, an ID number, location data, an online identifier or reference to one or more factors specific to the physical, physiological, genetic, mental, psychological, economic, cultural, political or social identity of that individual, including opinions from or about the individual. Personal Data also includes business information such as job title, office telephone or business mobile phone numbers and details about professional credentials.

(v) "**Processed**" or "**Processing**" means any operation or set of operations performed on Personal Data including collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

(vi) "**Special Categories of Data**" are Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for the purpose of uniquely identifying a Data Subject, health, gender identification, sex life or sexual orientation. This is may be held in the context of employee Personal Data or claimant Personal Data. Personal Data relating to criminal offenses or alleged offenses and criminal proceedings ("**Criminal Offense Data**") is a Special Category of Data for purposes of this Policy.

4.2 Anonymous Data. This Policy does not require protection of any Data that is completely and truly anonymous.

4.3 Pseudonymous Data. Personal Data that is amended in such a way that no individual may be identified from the data (whether directly or indirectly) without a "key" that allows the data to be re-identified is known as "**Pseudonymous Data.**" That is, it is Personal Data that has been processed in such manner that the Personal Data can no longer be attributed to a specific Data Subject without the use of additional information. This Policy encourages the use of Pseudonymous Data wherever possible provided that (i) the "key" that enables re-identification of Data Subjects is kept separate and secure and (ii) the cost of converting the Data into Pseudonymous Data is justified by the reduction of the risk of a breach or improper disclosure of such Data compared to the risk without such data alteration.

4.4 Interpretation. The Chief Compliance Officer shall have responsibility for interpreting and applying these definitions to Sompo International's business in accordance with this Policy.

4.5 Identifying and Monitoring Processing Activities. Each business unit at Sompo International shall create and maintain a record of Processing that identifies and records Processing activities within and outside Sompo International, wherever located, and maintain an inventory of such Personal Data (each a "Record of Processing"). The Chief Compliance Officer shall coordinate an annual review of such Records of Processing.

4.6 Privacy Risk Assessment. The Chief Compliance Officer or his or her designee shall consult with all interested departments to ensure that appropriate data protection compliance measures and technical safeguards are established for each Processing activity, which shall include the following goals:

(i) identifies privacy risks at the outset of any project or before the implementation of a new product, system or service and plan for them accordingly;

(ii) uses Personal Data that is pseudonymised where possible and feasible;

(iii) embeds data protection and privacy concerns into the technologies, operations and information architectures of Sompo International;

(iv) maintains the integrity and high standards of Sompo International's products and services; and

(vii) strives for transparency with Data Subjects about protection of their Personal Data by Sompo International.

4.7 Privacy Impact Assessment. The Chief Compliance Officer shall design and implement procedures for a risk based evaluation of each new project, product, system or service considered by Sompo International. The procedures shall be designed to identify the potential adverse impact on

privacy concerns, including the rights of Data Subjects under applicable data protection and privacy laws and regulations. To the extent any such new project, product, system or service generates a high or unacceptable risk of such an adverse impact, then the procedures shall include measures for identifying appropriate mitigation measures, including safeguards and security measures, that protect Personal Data in compliance with applicable laws and regulations.

5.0 Protection and Use of Personal Data

5.1 Principles of Data Protection. This Policy requires Sompo International to:

(i) Process Personal Data in accordance with applicable laws and regulations (that is, lawfully processing Personal Data);

(ii) collect Personal Data for specific and legitimate purposes, including disclosure of such purposes to the Data Subject;

(iii) Process such collected Personal Data only in a way compatible with specific and legitimate purposes;

(iv) hold Personal Data for a retention period that is limited for the specific and legitimate business purposes for which it was collected and as necessary to comply with applicable laws and regulations;

(v) update Personal Data to maintain its accuracy;

(vi) secure Personal Data;

(vii) provide adequate protection for Personal Data that is transferred from the jurisdiction from which the Personal Data is derived to other jurisdictions in accordance with applicable laws and regulations; and

(viii) establish a framework of data protection that includes appropriate monitoring that confirms compliance with the foregoing.

5.2 Lawful Basis for Processing Personal Data. Personal Data may only be Processed by Sompo International in accordance with applicable law and regulations or, in other words, when Sompo International has a lawful basis to Process the Personal Data. Sompo International has a lawful basis to Process Personal Data if one of the following is satisfied:

(i) **Legitimate Business Interest.** Sompo International has a legitimate business interest to Process the Personal Data that is not overridden by the data protection rights of a Data Subject. Examples of legitimate business interests that are not overridden by a data protection right include underwriting or administering an insurance or reinsurance policy

or managing a claim arising under an insurance policy, and enforcing an employment arrangement;

(ii) **Compliance with a Legal Obligation.** Sompo International is Processing the Personal Data for the purpose of complying with a legal obligation under applicable laws or regulations;

(iii) **Performing a Contract.** Sompo International is performing its obligations under a contract including, but not limited to, an insurance or reinsurance contract; or

(iv) **Consent by the Data Subject.** When the Data Subject has properly given consent for the use and Processing of the Personal Data, Sompo International has a lawful basis for Processing the Personal Data.

5.3 **Lawful Basis for Processing Special Categories of Data.** Special Categories of Data, including Criminal Offense Data, may only be Processed in compliance with applicable laws and regulations. Any Processing of Special Categories of Data shall be subject to appropriate procedures and approved in advance by the Chief Compliance Officer or the Legal & Compliance Department

5.4 **Disclosure of purposes for Personal Data to Data Subject.** Sompo International shall disclose to Data Subjects how Sompo International will Process their Personal Data. Such disclosure shall be concise, transparent, intelligible and easily accessible, using clear and plain language. Sompo International shall include in such disclosure the following:

(i) the identity of the Chief Compliance Officer and provide pertinent contact information for communicating with the Chief Compliance Officer;

(ii) Sompo International's purposes and legal basis for Processing the Personal Data;

(iii) the recipients or categories of recipients of the Personal Data outside Sompo International;

(iv) details about transferring Personal Data outside the Data Subject's jurisdiction and the safeguards that are in place to protect such Personal Data;

(v) the retention periods or the criteria used to determine retention periods;

(vi) the Data Subject's data protection and privacy rights;

(vii) if the Data Subject's consent is the lawful basis of the Processing of the Personal Data, then the Data Subject has the right to withdraw consent at any time;

(viii) the Data Subject's right to complain to a government authority that has jurisdiction over data protection rights;

(ix) if providing the Personal Data is required by an applicable law or regulation, then referencing the Data Subject's legal obligation to provide it and possible consequences

for the Data Subject's failing to provide it;

(x) if automatic decision making is used, then disclosure about the logic involved in such automation, the significance of such automatic decision and the envisaged or potential consequences of such automated decision making;

(xi) if Sompo International does not receive the Personal Data directly from the Data Subject, then the following additional disclosures shall be made to the Data Subject: (A) the categories of Personal Data that Sompo International is collecting and (B) the source and, if applicable, whether it came from publicly accessible sources.

5.5 Timing of Disclosures. Such disclosure shall be made at the time the Personal Data is obtained from the Data Subject. If the Data Subject does not provide the Personal Data, then the disclosure shall be made to the Data Subject:

(i) within a reasonable period after obtaining the Personal Data, but at the latest one month;

(ii) if the Personal Data is used to communicate with the Data Subject, at the latest when the first communication takes place; or

(iii) if the disclosure to another recipient is planned or foreseeable, at the latest before the Personal Data is disclosed to such recipient.

5.6 Exceptions to Disclosure – Impossibility or Disproportionate Effort Required. If disclosure is impossible or requires disproportionate effort, then Sompo International shall take appropriate measures to protect the individual's interests and the required disclosure shall be made generally in a public manner such as unrestricted accessibility on the Sompo International website.

5.7 Limited Use of Personal Data. Sompo International shall only use Personal Data for a purpose that has been disclosed to the Data Subject and is compatible with the original purpose that has been disclosed to the Data Subject.

5.8 Limited Collection of Personal Data. Sompo International shall only collect Personal Data to the extent necessary or relevant for the purposes for which it is collected and that is in compliance with applicable law and regulations (that is, for which it has a lawful basis).

5.9 Retention and Accuracy of Personal Data. If Personal Data is retained, then it shall only be retained to the extent necessary to comply with the lawful purpose for which it was collected or that is necessary for Sompo International to comply with applicable laws and regulations. To the extent

Personal Data is retained and used again, then Sompo International shall keep such Personal Data updated. Sompo International's Records Retention Policy shall be updated from time to time to incorporate the requirements of this Policy concerning retention of Personal Data, as this Policy changes from time to time.

5.10 Deleting or Erasing Records. Personal Data that is not required to be retained pursuant to this Policy or the Sompo International Records Retention Policy shall be deleted in a secure manner.

6.0 Security of Personal Data

6.1 Protection Against Unauthorized Processing or Use. Personal Data, wherever stored and whenever transferred, shall be protected against unauthorized or unlawful Processing and from accidental loss, destruction or damage in accordance with applicable laws and regulations and the Sompo International Information Security Policy.

6.2 Personal Data Breaches. A "**Personal Data Breach**" means and includes 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. Sompo International shall report each Personal Data Breach to the appropriate governmental authority to the extent required by and in accordance with all applicable laws and regulations within the time period required for such reporting. The Chief Compliance Officer shall maintain a schedule of each jurisdiction that has laws or regulations applicable to Sompo International and the threshold and reporting requirements for a Personal Data Breach, including deadlines for submitting the report. If at any time, any employee or consultant of Sompo International becomes aware of a Personal Data Breach, such employee or consultant shall immediately report the breach to the Chief Compliance Officer, local compliance or privacy officer or other member of the Legal & Compliance Department. The Chief Compliance Officer then shall determine the appropriate response and follow-up based upon the risk and severity of the breach, including notifications as required by applicable law or otherwise deemed appropriate by the Chief Compliance Officer.

7.0 Application of this Policy to Vendors and Service Providers

7.1 Application to Data Processors. This Policy shall apply to all Data Processors. All Data Processors shall comply with this this Policy.

7.2 Oversight and Audit of Data Processors. Each employee of Sompo International who has responsibility for overseeing or managing a Data Processor shall coordinate with the Chief Compliance Officer with respect to confirmation of compliance with this Policy by such Data Processor. Each such employee and the Chief Compliance Officer shall include in the oversight and supervision of such Data Processor an appropriate audit that confirms that such Data Processor has the capabilities and has implemented the appropriate technical, organizational and relevant requirements and measures to comply with this Policy. Such audit and confirmation shall also confirm that the Data Processor is complying with the data protection and privacy rights of Data Subjects under applicable law.

7.3 Required Contract Provisions. Each contract between a Data Processor and Sompo International shall include the provisions, terms and conditions that incorporate the requirements of this Policy and applicable laws and regulations. The Legal & Compliance Department shall maintain and keep updated the required contractual provisions for each jurisdiction to which the Data Processor is subject and assist each employee who has responsibility for such contract with the appropriate procedures for ensuring that the contractual requirements that apply to such Data Processors comply with the requirements of this Policy and applicable laws and regulations, as this Policy and such laws and regulations are updated from time to time.

8.0 Training and Continuing Education

The Chief Compliance Officer shall coordinate with the applicable departments within Sompo International to provide adequate training about the requirements of this Policy and other Sompo International policies concerning information security for all personnel as part of the functions and operations they perform on behalf of Sompo International.

9.0 Audit and Oversight

Sompo International's Internal Audit Department and the Audit and Governance Committee of Sompo International's Board of Directors shall have primary responsibility for overseeing the auditing of Sompo International's operations for the purpose of confirming compliance with this Policy, including compliance with the Sompo International Information Security Policy.

10.0 Amendment of this Policy

10.1 This Policy may not be amended without the prior approval of the Board of Directors of Sompo International (the "**Board of Directors**") either on its own or as delegated to a committee of the Board of Directors, except as set forth below.

10.2 The Chief Compliance Officer shall have authority to implement a change of this Policy immediately, on a temporary basis, without first receiving the approval of the Board of Directors provided that (i) such change does not change the overall purposes or goals of this Policy, (ii) such change is for the purpose of complying with an applicable law or regulation, or (iii) such change is for the purpose of improving the administration or implementation of this Policy or to more effectively or efficiently achieve the overall purposes or goals of this Policy. If so amended, the Chief Compliance Officer thereafter shall notify the Board of Directors of such change at the next regularly scheduled meeting of the Board of Directors and obtain the approval of such Board of Directors to make such change a permanent change. Even if the Board of Directors, however, disapproves making such change a permanent change, the Chief Compliance Officer's decision to make the temporary change shall be deemed a temporary amendment of this Policy that was in effect during the period prior to the disapproval of the Board of Directors.