Blue Cross 藍十字
An AIA Company 友邦保險成員公司

中國內地私隱協議附錄
（「本私隱附錄」）

本私隱附錄僅於閣下位於中國內地時適用。

作為閣下的保單繕發機構或「至醒會」管理者，藍十字（亞太）保險有限公司（以下簡稱「**我們**」）是閣下個人資料的控制者和處理者，閣下可以經以下地址與我們的資料保障主任聯繫：

香港灣仔皇后大道東 183 號合和中心 54 樓
藍十字（亞太）保險有限公司
資料保障主任

本私隱附錄構成我們的《個人資料收集聲明》的組成部分，並僅適用於位於中國內地並接收我們從香港提供的產品及／或服務的個人客戶（包括作為公司客戶的個人董事和僱員）。根據中國內地法律的要求，我們可能需要就如何使用閣下的個人資料取得閣下的同意，及對於某些基於中國內地法律被視為敏感的個人資料，我們可能需要取得閣下的獨立同意。閣下的個人資料將被收集、存取、處理、使用、儲存及／或轉移至中國內地境外。如果閣下不同意本私隱附錄，我們可能無法向閣下提供閣下購買的產品，並且無法向閣下提供與該產品相關的服務，這亦包括在閣下（作為僱員）不同意本私隱附錄情況下，我們將無法向公司客戶（即閣下的僱主）提供產品或服務。

根據中國內地適用的資料保護法律，我們將基於閣下的同意處理閣下的個人資料，除非閣下的個人資料屬於以下情況：

- 為訂立或履行由閣下作為其中一方當事人的合約所必須的；
- 為我們履行法定義務所必須的；
- 為應對突發公共衛生事件所必須的；
- 為保護個人的生命、健康和財產安全所必須的；
- 為公共利益，進行新聞報導、輿論監督行為在合理範圍內處理的個人資料；及
- 由於閣下自行披露或因法律要求，及已經合理地處理的公開個人資料。

我們收集閣下的特定個人資料部分屬於中國內地的適用資料保護法律所定義的敏感個人資料（以下簡稱「**敏感個人資料**」），即如果被洩露或被非法使用，可能對閣下的權利及利益產生重大影響的個人資料，包括但不限於財務帳戶、身份證件號碼、健康相關資料或未滿 14 週歲未成年人的任何個人資料。我們收集敏感個人資料僅用於特定目的，例如評估閣下的保單申請以繕發保單，及調查閣下向我們提交的任何索賠申請。

我們將在必要時限內保留閣下的個人資料，以實現我們的《個人資料收集聲明》和本私隱附錄所述目的。我們將通過以下一項或多項的因素來決定閣下個人資料的保存期限：我們是否與閣下仍有持續關係；根據我們必須遵守的法律義務要求；以及依據我們的法律地位來決定（例如適用的訴訟時效、訴訟、審計或監管調查）。

為了管理閣下的保單以及向閣下提供產品和服務，我們也可能將閣下的個人資料提供給我們的代理人、經紀、承保人、承包人、閣下的僱主、第三方服務供應商、醫療機構例如醫院、診所以及實驗室測試設施，母公司、附屬公司和聯屬公司、核數師、法律顧問、團體保險公司客戶（包括其成員公司）及該團體保險下接受我們的保險產品及服務的閣下和閣下的家屬、財務顧問、再保險公司、監管機構、政府、稅務、執法或其他機關、或自律監管機構或行業組織或協會、我們的權利或業務的實際或建議承讓人、受讓人、參與人或附屬參與人、銀行，支付結算代理人，第三方支付服務提供者、索賠調查機構、第三方獎賞、客戶或會員、品牌合作及優惠計劃供應商、品牌合作夥伴及／或營銷夥伴、保險核算人、醫護專業人士、會計師、財務顧問、律師、整合保險業申索和承保資料的組織、防欺詐組織、其他保險公司、警察、及保險業就使用現有資料而對所提供的資料作出分析和檢查的數據庫或登記冊（以下稱「**接收方**」）。此外，我們可能會向某些接收方提供閣下的個人資料，這些接收方可以獨立決定與閣下的個人資料處理活動相關的目的和方式。個人資料接收方名單可在這名單查閱。

閣下的個人資料的接收方可以收集和處理閣下的個人資料，並將其交還給我們，以便我們管理閣下的保單及向閣下提供產品及服務。我們向接收方提供的個人資料類型包括但不限於：個人識別資訊、閣下的醫療資料、閣下的健康記錄／資料及財務資料。我們可以通過電子或其他方式向接收方提供閣下的個人資料。我們在控制、處理和轉移閣下的個人資料和敏感個人資料時，將採取最高的安全措施，以符合中國內地適用的法律及法規。我們亦採用自己的安全政策以保護閣下的個人資料和敏感個人資料。

在我們開展業務時，我們可能會使用人工智慧處理閣下的個人資料以實現收集閣下的個人資料的用途。人工智慧是一種模擬人類思考過程來感知、理解、推理和解決問題以增強、改進或取代人類決策的技術。使用人工智慧的常見例子包括：

- 客戶互動－自然語言處理將語音轉換為文字並與客戶進行適當的互動；
- 數據化申請和服務流程－使用光學字元辨識工具於申請和服務流程，該工具可識別數位影像中的文字，並驗證根據文件填寫的表格之準確性；及
- 產品及產品組合推薦－將人工智慧用於我們的客戶資料庫並進行大數據分析，使我們能夠了解客戶的需求。

除我們的《個人資料收集聲明》中闡述的查閱及改正資料權利外，閣下亦有權取得我們持有閣下的個人資料的副本，並有權在下列任何情形發生時要求我們刪除閣下的個人資料：

- 處理閣下的個人資料的目的已經達到或未能達到，或該個人資料對於達到該目的已無必要；
- 我們已停止提供產品或服務，或保留期限已屆滿；
- 閣下已撤回同意；及
- 我們違反了資料保護適用的法律及法規。

如果與本私隱附錄的條款不一致時，包括但不限於定義（例如敏感個人資料），則以中國《網絡安全法》、《個人信息保護法》、《數據安全法》、其實施措施和其他網絡安全和資料保護相關的中國內地法律及法規為準。

我們有權不時更新本私隱附錄，並通過我們網站或應用程式（視乎情況而定）發佈本私隱附錄的更新以向閣下通知相關內容。閣下可以通過我們的《個人資料收集聲明》中列出的聯繫方式與我們聯繫，以撤回對我們處理閣下個人資料的同意。如果閣下撤回對我們處理閣下的個人資料的同意，我們可能無法向閣下提供相關產品及／或服務。

（202504）

Blue Cross 藍十字
An AIA Company 友邦保險成員公司

Privacy Addendum for mainland China
(this "Privacy Addendum")

This Privacy Addendum only applies to you if you are located in mainland China.

Blue Cross (Asia-Pacific) Insurance Limited (hereinafter referred to as "**we**", "**us**" or "**our**"), the issuer of your insurance policy or administrator of SmartClub, is the controller and processor of your personal data and you may reach us by writing to our Data Protection Officer at the following address:

The Data Protection Officer
Blue Cross (Asia-Pacific) Insurance Limited
54/F, Hopewell Centre
183 Queen's Road East
Wanchai, Hong Kong

This Privacy Addendum forms part and parcel of our Personal Information Collection Statement and is specific to individual customers (including individual directors and employees of a corporate customer) who are located in mainland China and receiving our products and/or services from Hong Kong. As required by the laws of mainland China, we may need to seek your consent on how we use your personal data and, in relation to certain personal data which is considered sensitive based on the laws in mainland China, we may need your separate consent. Your personal data will be collected, accessed, processed, used, stored, and/or transferred outside of, mainland China. If you do not consent to this Privacy Addendum, we may not be able to provide you with the product(s) you are purchasing from us and offer you with the services associated with the product(s) and this would also include our inability to provide products or services to a corporate customer which is your employer if you (as an employee) do not consent to this Privacy Addendum.

Under the applicable data protection laws in mainland China, we will process your personal data based on your consent, unless your personal data are:

- necessary to conclude or perform a contract in which you are a party;
- necessary for us to comply with legal obligations;
- necessary to respond to public health emergencies;
- necessary to protect individuals' life, health, and property safety;
- reasonably processed in news reporting and public opinion oversight for public interests; and
- publicly available, because of your voluntary disclosure or a legal requirement, and reasonably processed.

Certain personal data that we collect about you is sensitive personal data as defined in the applicable data protection laws in mainland China ("**Sensitive Personal Data**"), which is personal data that may materially impact your rights and interests, if breached or unlawfully used, including but not limited to financial accounts, identification number, health-related information, or any personal data of minors under the age of fourteen. We collect the Sensitive Personal Data only for specific purposes, such as assessing your application for the issuance of an insurance policy to you, and investigation on any claims applications submitted to us.

We will retain your personal data for the period necessary to fulfill the purposes outlined in our Personal Information Collection Statement and this Privacy Addendum. The criteria used to determine our retention periods may include one or more of the following: as long as we have an ongoing relationship with you; as required by a legal obligation to which we are subject; and as advisable in light of our legal position (such as in regard of the applicable statute of limitation, litigation, audits or regulatory investigation).

We may also provide your personal data with our agents, brokers, insurers, contractors, your employer, third party service providers, medical institutions such as hospitals, medical clinics and laboratory testing facilities, parent companies, subsidiaries and affiliated companies, auditors, legal advisors, corporate customers (including their member companies) who maintain group insurance policy with us and, under which policy, you and your dependants receive insurance products or services from us, financial advisors, reinsurers, regulators, governmental, tax, law enforcement or other authorities, or self-regulatory or industry bodies or associations, actual or proposed assignee, transferee, participant or sub-participant of our rights or business, banks, payment settlement agents, third party payment service providers, claims investigation organizations, third party reward, loyalty, co-branding and privileges program providers, co-branding partners and/or marketing partners, insurance adjusters, health care professionals, accountants, financial advisors, solicitors, organizations that consolidate claims and underwriting information for the insurance industry, fraud prevention organizations, other insurance companies, the police and databases or registers (each, a "**recipient**", collectively, "**recipients**") for the purpose of the administration of your insurance policies, and the provision of products and services to you. Further, we may provide your personal data with certain recipients that can independently determine the purposes and means with respect to processing activities of your personal data. A list of such personal data recipients is available at this table.

The recipient(s) of your personal data may collect and process your personal data and return to us for the purpose of the administration of your insurance policies and the provision of products and services to you. The types of personal data that we provide to the recipients include without limitation personally-identifiable information, your medical information, your health records/information, your financial information. We may deliver your personal data through electronic means or other mode of dispatch to the recipients. In compliance with the applicable rules and regulations of mainland China, we implement maximum security in controlling, processing and transferring of your personal data and Sensitive Personal Data. We also adopt our own security policies to safeguard your personal data and Sensitive Personal Data.

While we carry out our business, we may use Artificial Intelligence ("**AI**") to process your personal data to fulfil the purposes of collecting your personal data. AI is a technology to simulate the human thought process to perceive, understand, reason and solve problems to augment, improve, or replace human decisions. Common examples for using AI include:-

- Customer interaction – natural language processing that converts voice to text and conducts appropriate interaction with customers;
- Digital onboarding and servicing processes – application and servicing processes using optical character recognition tool that recognizes text within digital images and validates the accuracy of form contents filled out against the supporting documents; and
- Product and portfolio recommendation – AI is used to conduct big data analysis based on our customer database and enables us to understand the needs of our customers.

In addition to the access and correction rights set forth in our Personal Information Collection Statement, you have the right to obtain a copy of your personal data held by us and the right to request us to delete such personal data under any of the following circumstances:

- where the purposes of processing your personal data have been achieved or have failed to be achieved, or the personal data is no longer necessary for achieving the purposes;
- where we have ceased to provide the products or services, or the retention period has expired;
- where you have withdrawn your consent; and
- where we have violated the applicable data protection laws and regulations.

To the extent inconsistent with the provisions of this Privacy Addendum, including but not limited to definitions (e.g., sensitive personal information), China's Cybersecurity Law, Personal Information Protection Law, Data Security Law, their implementing measures and other Chinese laws and regulations in relation to cybersecurity and data protection will prevail.

We have the right to update this Privacy Addendum from time to time and we will notify you of our updates to this Privacy Addendum by posting it on our website or apps (as the case may be). You may withdraw your consent to our use of your personal data by contacting us through the contact details set out in our Personal Information Collection Statement. If you withdraw your consent to our processing of your personal data, we may not be able to provide the relevant products and/or services to you.

(202504)