**ANNEXURE A**

**PERSONAL INFORMATION PROCESSING ADDENDUM TO THE SUPPLEMENTARY AGREEMENT IN RESPECT OF THE APPOINTMENT OF A**

**GROUP LIFE INSURER**

**PREAMBLE**

This Addendum –

1. serves as the written agreement between the Insurer as Operator and SARS as Responsible Party as contemplated in section 21 of POPIA;
2. sets out the specific terms and conditions on which the Insurer must process Personal Information relating to the Supplementary Agreement; and
3. is an integral part of and must be read with the Supplementary Agreement.
4. **INTERPRETATION AND DEFINITIONS**
	1. In this Addendum, unless clearly inconsistent with or otherwise indicated by the context:
		1. “**Addendum**” means this Personal Information processing addendum;
		2. “**Contractual Purposes**”means the exclusive purpose for which the Insurer may lawfully process Personal Information furnished by SARS in terms of the Supplementary Agreement, which is the execution by the Insurer of the Services;
		3. “**Supplementary Agreement**”means the Supplementary Agreementconcluded between the Parties in respect of Group Life Insurance Services procured by SARS from the Insurer pursuant to RFP 39/2024;
		4. “**Operator**” is as defined in POPIA, and in this Addendum, specifically refers to the Insurer;
		5. “**Personal Information Breaches**” means the accidental, unauthorised, or unlawful processing, access, copying, modification, reproduction, display or distribution of Personal Information, including the accidental or unlawful loss, destruction, alteration, disclosure and damage of or to Personal Information;
		6. “**Process**” **and/or “Processing**” is as defined and contemplated in POPIA; and
		7. “**Responsible Party**” is as defined in POPIA, and in this Addendum, specifically refers to SARS.
	2. Unless a definition is expressly amended herein, words and phrases defined in the Supplementary Agreement shall bear the same meaning in this Addendum, and in the event of there being a conflict between the terms and conditions of the Supplementary Agreement and those of this Addendum, the provisions of this Addendum shall prevail and take precedence, in so far as the conflict relates to matters which are the subject of this Addendum.
	3. Terms / Wording defined in POPIA and used in this Addendum bear definitions contained in POPIA, except where otherwise defined or amplified herein.
	4. The principles of interpretation stated in the Supplementary Agreement apply to this Addendum.
5. **INSURER’S OBLIGATIONS IN RELATION TO PERSONAL INFORMATION**
	1. **General Obligations**

The Insurer must –

* + 1. process Personal Information only to the extent, and in such a manner, as is necessary for the Contractual Purposes;
		2. not process Personal Information for any other purpose or in a way that does not comply with this Addendum; the Supplementary Agreement; POPIA or other Applicable Law;
		3. where SARS issues an instruction to the Insurer and the Insurer is of the view that such instruction is inconsistent with POPIA or other Applicable Law, the Insurer must immediately notify the SARS Authorised Representative, and await SARS’ written response on the pertinent issue;
		4. immediately comply with any written instructions by SARS to stop processing any Personal Information; and
		5. where required, assist SARS at no additional cost, with meeting SARS’ regulatory compliance obligations under POPIA in so far as such compliance relates to or is in connection with the Services or Personal Information provided to the Insurer by SARS.
	1. **Obligations relating to the Insurer’s Personnel**
		1. The Insurer must ensure that the Insurers’ Personnel –
1. are informed of the confidential and sensitive nature of Personal Information;
2. are bound by written confidentiality / information protection obligations, and have in place limitations of access or access restrictions in respect of Personal Information;
3. have undertaken training on POPIA and understand how it relates to their handling of Personal Information and how it applies to their duties; and
4. are aware of both the Insurer’s duties and obligations, and their personal duties and obligations under POPIA and the Supplementary Agreement.
	* 1. The Insurer must, as necessary, conduct background checks consistent with Applicable Law and take reasonable steps to ensure the reliability, integrity and trustworthiness of the Insurer’s Personnel with access to Personal Information.
	1. **Obligations relating to Information Security Measures**
		1. The Insurer must, as of the Effective Date, implement security measures and maintain in place, for the duration of the Supplementary Agreement, appropriate technical and organisational measures as contemplated in section 19 of POPIA to protect Personal Information and prevent Personal Information Breaches. Such measures must provide a level of security commensurate with corresponding risks, and may, as appropriate, include –

(a) the pseudonymisation and encryption of Personal Information;

(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

(c) the ability to restore the availability and access to Personal Information in a timely manner in the event of a physical or technical incident; and

(d) processes for regularly testing, assessing and evaluating the effectiveness of the security measures.

* + 1. The Insurer must immediately, in writing, notify the SARS Authorised Representative at their provided email addresses, as well as the SARS Contracts Management office at the email address: Proc.OPE@sars.gov.za (Attention: Contracts Management), and the SARS Anti-Corruption Unit at the email address: Anti-Corruption@sars.gov.za, where the Insurer or the Insurer’s Personnel have reasonable grounds to believe or suspect that there has been a Personal Information Breach in respect of any Personal Information processed or held by the Insurer pursuant to this Agreement.
		2. Immediately following any Personal Information Breach, the Parties must meet to discuss the matter as necessary. The Insurer must, at no additional cost, co-operate with and assist SARS in its further handling of the matter, including but not limited to:

(a) assisting with any investigation;

(b) providing SARS with physical access to any facilities and operations affected;

(c) facilitating interviews with the Insurer’s Personnel, including former employees and other parties involved in the matter;

(d) making available all relevant records, logs, files, Personal Information reporting and other material required to comply with POPIA or as otherwise reasonably required by SARS; and

(e) taking reasonable and prompt steps to mitigate the effects and to minimise any damage resulting from the Personal Information Breaches.

* 1. **SARS’ Audit Rights**
		1. The Parties recognise that compliance with POPIA is material and critical to the successful implementation of the Supplementary Agreement. SARS will, as part of honouring its legislative obligations as Responsible Party and as a POPIA compliance risk management strategy on its part, be entitled to monitor and audit the Insurer’s compliance with the Supplementary Agreement, in general, and to conduct *ad hoc* audits of the Insurer’s compliance with this Addendum, to ensure that the Insurer as Operator is fully compliant with the necessary POPIA, and contractual imperatives set out herein.
		2. In addition to SARS’ rights contemplated in the Supplementary Agreement, SARS will be entitled to take any other reasonable monitoring measures to satisfy itself that Personal Information, its employees, and stakeholders are not exposed to any risk of non-compliance with POPIA: Provided that any such measures will be implemented within the confines of Applicable Law, with prior notification to the Insurer.
	2. **Data subject requests and third-party rights**
		1. The Insurer must, at no additional cost to SARS, take such technical and organisational measures as may be appropriate, and promptly provide such information to SARS, as may reasonably be required, to enable SARS to comply with:
1. the rights of a data subject under POPIA; including, but not limited to, data subject access rights, the rights to rectify, port and erase Personal Information, object to the processing and automated processing of Personal Information, and restrict the processing of Personal Information; and
2. any notice or request from a Regulatory Authority in relation to POPIA.
	* 1. The Insurer must promptly notify SARS in writing where it receives any complaint, notice or communication that relates directly or indirectly to the processing of Personal Information or to either Party’s compliance with POPIA.
		2. The Insurer must notify SARS within twenty-four (24) hours where it receives a request from a data subject for access to their Personal Information or to exercise any of their other rights under POPIA.
		3. The Insurer must further provide, at no additional cost to SARS, its full co-operation and assistance in responding to any complaint, notice, communication or data subject request.

* 1. **Indemnity**
		1. The Insurer agrees to, at its own expense, indemnify, keep indemnified and defend SARS against all Losses incurred by SARS or for which SARS may become liable due to any failure by the Insurer or the Insurer’s Personnel, to comply with any of the Insurer’s obligations under this Addendum and/or POPIA.