



Contents

FSCA RF Notice 8 of 2025 – Exemption of Retail Funds in relation to Amalgamations and Transfers from the Requirements of Section 14(1) of the Pension Funds Act, 1956 (Act No 24 of 1956) – 14 July 2025

Joint Communication 2 of 2025: Cloud Computing and Data Offshoring – 25 July 2025

Joint Communication 3 of 2025: For consultation: Determination of the notification template in terms of Joint Standard 1 of 2023 – IT Governance and Risk Management for Financial Institutions and Joint Standard 2 of 2024 – Cybersecurity and Cyber Resilience Requirements for Financial Institutions – 3 September 2025

Legal & industry update – September 2025

In this publication we look at:

- FSCA RF Notice 8 of 2025 – Exemption of Retail Funds in relation to Amalgamations and Transfers from the Requirements of Section 14(1) of the Pension Funds Act, 1956 (Act No 24 of 1956)
- Joint Communication 2 of 2025: Cloud Computing and Data Offshoring
- Joint Communication 3 of 2025: For consultation: The notification templates in terms of Joint Standard 1 of 2023 (IT Governance and Risk Management for Financial Institutions) and Joint Standard 2 of 2024 (Cybersecurity and Cyber Resilience Requirements for Financial Institutions)

FSCA RF Notice 8 of 2025 – Exemption of Retail Funds in relation to Amalgamations and Transfers from the Requirements of Section 14(1) of the Pension Funds Act, 1956 (Act No 24 of 1956) – 14 July 2025

After a consultation process following Communication 14 of 2025, the FSCA issued RF Notice 8 of 2025, formally exempting retail retirement funds from the requirements of section 14(1) of the Pension Funds Act (PFA).

This exemption applies to retail funds such as retirement annuity (RA) funds, pension preservation funds and provident preservation funds.

The exemption allows transfers:

•
•

between
RA funds

between
preservation
funds

from
preservation
funds to RA
funds

without fully following section 14(1), but only if these specific conditions are met:

- a. the records of any transaction effected must be maintained by both retail funds and be made available to the Authority if requested;
- b. the proposed transaction may only be effected in terms of the rules of the relevant funds and the provisions of such rules must be complied with;
- c. the relevant forms, as determined by the Authority, have been completed; and certified;
- d. the following documents are kept on file in respect of the transfer:
 - (i) proof that the proposed transaction has been communicated and that any objections have been addressed; and
 - (ii) proof that the Authority is satisfied that the requirements for surplus schemes in terms of section 15B of the Pension Funds Act have been complied with (where applicable)
- e. the assets and liabilities are transferred within 180 days of the effective date of transfer; and
- f. any assets transferred must be increased or decreased with fund return from the effective date until the date of final settlement.

The exemption aims to reduce administrative burdens while ensuring proper oversight and safeguarding retirement fund members' interests during transfers.

Joint Communication 2 of 2025: Cloud Computing and Data Offshoring – 25 July 2025

On 25 July 2025, the FSCA and Prudential Authority released Joint Communication 2 of 2025, signalling plans to draft a Joint Standard with clear rules for cloud use and data offshoring. This guidance emphasises the role of boards and senior management in managing risks tied to these technologies.

Cloud computing is considered a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage facilities, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

Source: Joint Communication 2 of 2025

The offshoring of data is the storage and/or processing of data outside the borders of South Africa.



The Joint Communication proposes that, when implementing any cloud computing and/or data offshoring solution, financial institutions should:

- Apply risk-based strategies tailored to their business size and complexity.
- Consider establishing strong governance structures, processes and procedures. These could include, for example, formulating a defined policy, board-approved data strategy and data governance framework that addresses the financial institution's risk appetite for cloud computing and/or data offshoring.
- Take all reasonable measures to ensure the confidentiality, integrity and availability of their data, information technology applications or systems.
- Consider contractual and other legal requirements for these services and the enforceability of rights and obligations arising from these contractual arrangements.
- Exercise appropriate due diligence before investing in the use of cloud computing and/or offshoring.

While the full scope of institutions affected is still under review, the authorities plan to publish the draft standard for public consultation in due course. Supervisory oversight on cloud computing and offshoring risks will intensify through 2025 and 2026 as part of regular supervision efforts, aiming to protect the financial sector and align with global best practices.

Joint Communication 3 of 2025: For consultation: Determination of the notification template in terms of Joint Standard 1 of 2023 – IT Governance and Risk Management for Financial Institutions and Joint Standard 2 of 2024 – Cybersecurity and Cyber Resilience Requirements for Financial Institutions – 3 September 2025

Joint Communication 3 of 2025, issued for consultation on 3 September 2025, introduces a draft notification template for financial institutions to comply with Joint Standard 1 of 2023 (IT Governance and Risk Management) and Joint Standard 2 of 2024 (Cybersecurity and Cyber Resilience).

The Communication standardises how institutions report IT governance, risk management, cybersecurity incidents and cyber resilience measures to the Financial Sector Conduct Authority (FSCA) and Prudential Authority. You can view the reporting template [here](#).

Its goal is to improve regulatory oversight, enhance operational and cyber risk management, and ensure consistent, timely incident reporting to strengthen the financial sector's resilience against IT and cyber threats. Institutions and stakeholders are invited to comment on the proposed template.

Comments are due on the templates by 5 October 2025.

This publication does not provide advice or legal opinion. If you have any questions/comments on the above, please contact your consultant.

Aon South Africa (Pty) Ltd, Actuarial, Healthcare & Retirement Fund Consultants
The Place, 1 Sandton Drive, Sandhurst, Sandton, 2196
P O Box 78367, Sandton, 2146
+27 11 944 7000 | www.aon.co.za
© Aon Corporation, 2022. All rights reserved

Aon South Africa (Pty) Ltd is an Authorised Financial Services Provider | License # 20555.
Aon Limpopo (Pty) Ltd, an authorised Financial Services Provider, FSP # 12339

This report (including all its contents) is intended as a management tool to give you a high level overview of some of the salient aspects of your portfolio, but should not be relied upon as making any recommendations or providing advice to you. The content of this bulleting and information provided may be of a general nature. It is therefore recommended that you obtain appropriate legal, tax, investment or other professional advice for the formulation of an appropriate investment strategy. Any decisions regarding your portfolio should be made in consultation with you Aon client relationship manager. The report contains information which has been obtained from a number of sources and contains a mix of historical, current or future assumptions as at a specific date and may vary from the date of publication. These assumptions/ projections are estimates and are subject to change. While Aon has taken responsible steps to ensure that the information contained in this report is relevant, accurate and current, no warranties of any kind, whether express or implied, including but not limited to the accuracy, completeness, relevance or fitness for a particular purpose are given and Aon expressly disclaims any liability for any loss or damage that may arise from the use of this report. This report is for your internal use only and may not be provided to any third party without Aon's prior written consent. Copyright ownership in this report (including all its contents) attaches strictly to Aon and may not be reproduced, alienated or disseminated in any way without the prior written consent of Aon.