South African Reserve Bank

Financial Surveillance Department

2020-10-01

Exchange Control Circular No. 10/2020

Offshoring and cloud computing

Authorised Dealers and Authorised Dealers in foreign exchange with limited authority are advised that during June 2019 a position paper outlining the views of the Financial Surveillance Department with regard to offshoring and cloud computing by Authorised Dealers and reporting entities was published for comments.

Based on the responses, some common themes were identified and the proposed policy document was updated to simplify the requirements and to provide more clarity on the fact that the position paper is only applicable to functions, services, business processes, data, infrastructure and systems of reporting entities as contemplated in terms of the Currency and Exchanges Manual for Authorised Dealers and Currency and Exchanges Manual for Authorised Dealers in foreign exchange with limited authority. See Annexure A for the signed copy of the 'Offshoring and cloud computing position paper'.

Requests for utilising offshoring and cloud computing will only be considered, on a case-by-case basis, upon the submission of a formal application to the Financial Surveillance Department. In addition to ensuring compliance with the requirements and assurances specified by the Financial Surveillance Department, reporting entities must also be in compliance with the requirements of all other regulatory and supervisory institutions as well as applicable legislation. Specific reference is made to the directive (D3/2018) and guidance notes (G5/2018) with regard to offshoring and cloud computing issued by the Prudential Authority of the South African Reserve Bank.

The ultimate responsibility for ensuring that the risks associated with offshoring and cloud computing are duly managed, vests with the relevant reporting entities. Failure to comply with any of the requirements outlined by the Financial Surveillance

Department may result in measures being taken by it as administrator of the exchange control system.

The following amendments have been made to the Currency and Exchanges Manual for Authorised Dealers:

A new subsection J.(D) has been inserted and the current sections J.(D) to J.(H) have been renumbered J.(E) to J.(I) respectively:

(D) Offshoring and cloud computing

(i) The Financial Surveillance Department is prepared to consider requests to authorise the following offshoring and cloud computing models relevant exclusively to data, infrastructure and systems, as contemplated in the Authorised Dealer Manual:

(a) offshoring within a reporting entity's international head office and/or group;

(b) cloud computing relating to data, infrastructure and systems;

(c) local outsourcing of data, infrastructure and systems; and

(d) real-time system and data replication to South Africa from an international head office and/or group.

(ii) The Financial Surveillance Department is not agreeable to the following offshoring and cloud computing models:

(a) offshoring, local and international outsourcing or cloud computing of functions, services and business processes as contemplated in the Authorised Dealer Manual; and

(b) any form of offshoring and cloud computing models where data is stored in a sanctioned country or in jurisdictions that may inhibit effective access to data.

(iii) Requests for utilising offshoring and cloud computing will only be considered, on a case-by-case basis, upon the submission of a formal application to the Financial Surveillance Department.

(iv) The following requirements must be adhered to:

(a) Agreements

(aa) A documented legally binding agreements or contracts must be concluded with the reporting entity's Head Office or any other third party that forms part of the proposed operating model. These agreements or contracts must state, but not be limited to, the following:

(1) data relevant to the reporting entity will be ring-fenced from other activities of the data centre to be used and should stipulate how it will be achieved;

(2) data will be retained for a minimum period of five years, as required by the Authorised Dealer Manual; and

(3) data will be accessible immediately, but not later than 48 hours, from the source systems and extractable in the format prescribed in (h)(gg) below.

(bb) Any amendments to the above agreements/contracts with regard to a change in the approved operating model requires prior approval of the Financial Surveillance Department.

(b) Risk assessment

(aa) Prior to undertaking a particular offshoring and cloud computing initiative, a reporting entity must perform a risk assessment, which must be documented.

(bb) The risk assessment must identify all risks involved and determine whether adequate controls can be implemented to mitigate any potential risks.

(cc) A reporting entity must have documented processes and procedures in place to, on a continuous basis identify, assess, manage and mitigate risks associated with offshoring and cloud computing.

(dd) Risks must be adequately understood and managed prior to entering into an offshoring and cloud computing arrangement. Factors that must be addressed include, inter alia, continuity, data protection, regulatory access to data and regulatory compliance.

(c) Business continuity plan

(aa) A reporting entity must satisfy itself that the data centre hosting the data must have extensive disaster recovery and business continuity processes and procedures in place.

(bb) Regular disaster recovery tests must be performed to ensure data can be recovered.

(d) Storage of data

(aa) All data must be ring-fenced without the ability to be updated by unauthorised persons.

(bb) Cross-border transactional data must be stored directly into the source system, i.e. the core accounting system.

(cc) Customer data must be stored directly from the source system, i.e. the centralised customer database.

(dd) In an event of the reporting entity terminating its operations in South Africa for any reason whatsoever, data for five years preceding the date of termination, must be replicated to South Africa by the reporting entity in a format accessible by the Financial Surveillance Department and within an agreed period.

(e) Regulatory access to data

(aa) Any data required by the Financial Surveillance Department must be made available for access immediately, but not later than 48 hours, by the reporting entity and should forthwith be furnished to the Financial Surveillance Department in the format prescribed in paragraph (h)(gg) below.

(bb) Information must be made available, upon request, at no cost to the Financial Surveillance Department.

(cc) The use of offshoring and cloud computing may not in any way infringe on the Financial Surveillance Department's mandated access to data.

(f) Jurisdiction

(aa) A reporting entity must ensure that data is not stored in a sanctioned country or in jurisdictions that may inhibit effective access to data.

(bb) In considering foreign jurisdictions, a reporting entity must take into account the wider political and security stability of the particular jurisdiction as well as the legislative requirements in terms of the foreign jurisdiction concerned. This should include consideration of the legal enforcement provisions within a jurisdiction.

(g) Procedure to update data back to source

(aa) From time to time a reporting entity may be required to amend certain data, e.g. balance of payments categories or cancel the reporting of a transaction. This might have an impact on the same source reporting principle, as all changes must be updated back to the source, i.e. transactional or accounting system.

(h) System requirements

(aa) Data in any offshore data centre must at the least be encrypted through modern encryption technology.

(bb) All cryptographic keys used in a storage encryption solution must be secured and managed properly to support the security of the solution.

(cc) To prevent the non-recovery of encrypted data, extensive planning of key management processes, procedures, and technologies should be performed before implementing storage encryption technologies. This planning should include all aspects of key management, including key generation, use, storage, recovery and destruction.

(dd) Only authorised personnel and systems must be able to retrieve, decrypt and process data through any network or cloud.

(ee) The foreign service provider should have very strong, documented and tested cyber controls to protect data against cybercrime.

(ff) A reporting entity must verify adherence to the agreed information security requirements, i.e. through third party assurance audits and/or any other security testing

requirements such as vulnerability scanning and penetration testing.

(gg) Data requested by the Financial Surveillance Department should be provided in a standard report format, as prescribed in the Authorised Dealer Manual, such as a semi-colon delimited file (e.g.CSV).

(i) Other regulatory bodies and legislative requirements

(aa) A reporting entity must consider the offshoring and cloud computing models in the context of its overarching regulatory obligations, which may include obligations to the Financial Intelligence Centre and the Prudential Authority who have different statutory objectives and may, therefore, have different requirements.

(bb) A reporting entity must acquaint itself with the relevant provisions of the applicable legislation, e.g. the Protection of Personal Information Act, 2013 (Act No. 4 of 2013) and Financial Intelligence Centre Act, 2001 (Act No. 38 of 2001).

(v) Applications to the Financial Surveillance Department should, inter alia, include the following:

(a) confirmation that the reporting entity complies with the requirements and assurance set out in (iii) above and (v) below; and

(b) a copy of the business case which should outline, inter alia, the following:

(aa) proposed offshoring and cloud computing operating model;

(bb) details of all relevant offshoring and cloud computing third parties or service providers;

(cc) benefits and risks involved;

(dd) confirmation that the management and mitigation of risks is done in order to maximise the benefits through effective end-to-end governance practices;

(ee) jurisdictions where data will be stored;

(ff) service, deployment and security models of offshoring and cloud computing applicable to the different classifications of data;

(gg) how data loss and breaches will be dealt with;

(hh) procedure to ensure that the reporting requirements stated in the Authorised Dealer Manual are adhered to;

(ii) procedures to be implemented to accommodate requests to update data from the source systems; and

(jj) strategy to be implemented in the event that offshoring and cloud computing operations are required to be moved from one provider to another.

(vi) Assurances

(a) The compliance with all the requirements listed in (iii) above, must be contained in the Managerial Letter of Comfort to be provided to the Financial Surveillance Department on an annual basis.

(vii) Remedies

(a) Any failure by a reporting entity to comply with the above mentioned requirements may result in the suspension of authorities provided by the Financial Surveillance Department or may cause the

Financial Surveillance Department to invoke remedies available to it in terms of the Exchange Control Regulations.

The following amendments have been made to the Currency and Exchanges Manual for Authorised Dealers in foreign exchange with limited authority:

A new subsection C.1(D) has been inserted and the current sections C.1(D) to C.1(H) have been renumbered C.1(E) to C.1(I) respectively:

(D) Offshoring and cloud computing

(i) The Financial Surveillance Department is prepared to consider requests to authorise the following offshoring and cloud computing models relevant exclusively to data, infrastructure and systems, as contemplated in the ADLA Manual:

(a) offshoring within a ADLA's international head office and/or group;

(b) cloud computing relating to data, infrastructure and systems;

(c) local outsourcing of data, infrastructure and systems; and

(d) real-time system and data replication to South Africa from an international head office and/or group.

(ii) The Financial Surveillance Department is not agreeable to the following offshoring and cloud computing models:

(a) offshoring, local and international outsourcing or cloud computing of functions, services and business processes as contemplated in the ADLA Manual; and

(b) any form of offshoring and cloud computing models where data is stored in a sanctioned country or in jurisdictions that may inhibit effective access to data.

(iii) Requests for utilising offshoring and cloud computing will only be considered, on a case-by-case basis, upon the submission of a formal application to the Financial Surveillance Department.

(iv) The following requirements must be adhered to:

(a) Agreements

(aa) A documented legally binding agreements or contracts must be concluded with the ADLA's Head Office or any other third party that forms part of the proposed operating model. These agreements or contracts must state, but not be limited to, the following:

(1) data relevant to the ADLA will be ring-fenced from other activities of the data centre to be used and should stipulate how it will be achieved;

(2) data will be retained for a minimum period of five years, as required by the ADLA Manual; and

(3) data will be accessible immediately, but not later than 48 hours, from the source systems and extractable in the format prescribed in (h)(gg) below.

(bb) Any amendments to the above agreements/contracts with regard to a change in the approved operating model requires prior approval of the Financial Surveillance Department.

(b) Risk assessment

(aa) Prior to undertaking a particular offshoring and cloud computing initiative, an ADLA must perform a risk assessment, which must be documented.

(bb) The risk assessment must identify all risks involved and

determine whether adequate controls can be implemented to mitigate any potential risks.

(cc) An ADLA must have documented processes and procedures in place to, on a continuous basis identify, assess, manage and mitigate risks associated with offshoring and cloud computing.

(dd) Risks must be adequately understood and managed prior to entering into an offshoring and cloud computing arrangement. Factors that must be addressed include, inter alia, continuity, data protection, regulatory access to data and regulatory compliance.

(c) Business continuity plan

(aa) An ADLA must satisfy itself that the data centre hosting the data must have extensive disaster recovery and business continuity processes and procedures in place.

(bb) Regular disaster recovery tests must be performed to ensure data can be recovered.

(d) Storage of data

(aa) All data must be ring-fenced without the ability to be updated by unauthorised persons.

(bb) Cross-border transactional data must be stored directly into the source system, i.e. the core accounting system.

(cc) Customer data must be stored directly from the source system, i.e. the centralised customer database.

(dd) In an event of the ADLA terminating its operations in South Africa for any reason whatsoever, data for five years

preceding the date of termination, must be replicated to South Africa by the ADLA in a format accessible by the Financial Surveillance Department and within an agreed period.

(e) Regulatory access to data

(aa) Any data required by the Financial Surveillance Department must be made available for access immediately, but not later than 48 hours, by the ADLA and should forthwith be furnished to the Financial Surveillance Department in the format prescribed in paragraph (h)(gg) below.

(bb) Information must be made available, upon request, at no cost to the Financial Surveillance Department.

(cc) The use of offshoring and cloud computing may not in any way infringe on the Financial Surveillance Department's mandated access to data.

(f) Jurisdiction

(aa) An ADLA must ensure that data is not stored in a sanctioned country or in jurisdictions that may inhibit effective access to data.

(bb) In considering foreign jurisdictions, an ADLA must take into account the wider political and security stability of the particular jurisdiction as well as the legislative requirements in terms of the foreign jurisdiction concerned. This should include consideration of the legal enforcement provisions within a jurisdiction.

(g) Procedure to update data back to source

(aa) From time to time an ADLA may be required to amend certain data, e.g. balance of payments categories or cancel

the reporting of a transaction. This might have an impact on the same source reporting principle, as all changes must be updated back to the source, i.e. transactional or accounting system.

(h) System requirements

(aa) Data in any offshore data centre must at the least be encrypted through modern encryption technology.

(bb) All cryptographic keys used in a storage encryption solution must be secured and managed properly to support the security of the solution.

(cc) To prevent the non-recovery of encrypted data, extensive planning of key management processes, procedures, and technologies should be performed before implementing storage encryption technologies. This planning should include all aspects of key management, including key generation, use, storage, recovery and destruction.

(dd) Only authorised personnel and systems must be able to retrieve, decrypt and process data through any network or cloud.

(ee) The foreign service provider should have very strong, documented and tested cyber controls to protect data against cybercrime.

(ff) An ADLA must verify adherence to the agreed information security requirements, i.e. through third party assurance audits and/or any other security testing requirements such as vulnerability scanning and penetration testing.

(gg) Data requested by the Financial Surveillance Department should be provided in a standard report format, as prescribed

in the ADLA Manual, such as a semi-colon delimited file (e.g.CSV).

(i) Other regulatory bodies and legislative requirements

(aa) An ADLA must consider the offshoring and cloud computing models in the context of its overarching regulatory obligations, which may include obligations to the Financial Intelligence Centre and the Prudential Authority who have different statutory objectives and may, therefore, have different requirements.

(bb) An ADLA must acquaint itself with the relevant provisions of the applicable legislation, e.g. the Protection of Personal Information Act, 2013 (Act No. 4 of 2013) and the FIC Act.

(v) Applications to the Financial Surveillance Department should, inter alia, include the following:

(a) confirmation that the ADLA complies with the requirements and assurance set out in (iv) above and (vi) below; and

(b) a copy of the business case which should outline, inter alia, the following:

(aa) proposed offshoring and cloud computing operating model;

(bb) details of all relevant offshoring and cloud computing third parties or service providers;

(cc) benefits and risks involved;

(dd) confirmation that the management and mitigation of risks is done in order to maximise the benefits through effective end-to-end governance practices;

(ee) jurisdictions where data will be stored;

(ff) service, deployment and security models of offshoring and cloud computing applicable to the different classifications of data;

(gg) how data loss and breaches will be dealt with;

(hh) procedure to ensure that the reporting requirements stated in the ADLA Manual are adhered to;

(ii) procedures to be implemented to accommodate requests to update data from the source systems; and

(jj) strategy to be implemented in the event that offshoring and cloud computing operations are required to be moved from one provider to another.

(vi) Assurances

(a) The compliance with all the requirements listed in (iv) above, must be contained in the Managerial Letter of Comfort to be provided to the Financial Surveillance Department on an annual basis.

(vii) Remedies

(a) Any failure by an ADLA to comply with the above mentioned requirements may result in the suspension of authorities provided by the Financial Surveillance Department or may cause the Financial Surveillance Department to invoke remedies available to it in terms of the Exchange Control Regulations.

The amended Currency and Exchanges Manual for Authorised Dealers and the Currency and Exchanges Manual for Authorised Dealers in foreign exchange with limited authority may be accessed on the SARB website: www.resbank.co.za by

following the links: Home>Regulation and supervision>Financial surveillance and exchange controls>Currency and exchanges documents.

Head of Department: Financial Surveillance