asifma
Growing Asia's Markets

ASIFMA Technology-Neutral Principles for Virtual Data Storage

June 2019

ASIFMA is pleased to present below principles for virtual data storage by firms licensed by (or registered with) financial regulators (collectively **regulated firms**). These principles reflect ASIFMA member consensus and were developed with the kind support of ASIFMA member firm EY.

We understand that some financial regulators in Asia are increasingly concerned about:

- how technological evolution in how regulatorily required data is stored with virtual storage of data now common, both on and off premises, and increasingly with third parties and cross-border, and
- that this has eroded its ability to exercise its existing powers under the law to obtain data from regulated firms with no or minimal risk of data being destroyed, hidden, or tampered with.

The principles are technology-neutral and aim to achieve certain outcomes important to ensure that regulated firms store all the data that the applicable laws and rules the financial regulator administers require to be stored in a regulatorily compliant manner. The principles are designed to help ensure that the financial regulator can continue to exercise its data gathering powers in relation to virtually stored data as much as reasonably and realistically possible as if it were exercising those powers against physically stored data within its home jurisdiction.

ASIFMA members suggest it is important for regulators to focus on outcomes rather than processes when looking at data storage, and advise against a "one size fits all" technical solution for all firms and business models. This will allow firms to apply a risk-based approach to compliance that is best-tailored to their specific business models and activities. Regulated firms are better positioned to understand their own systems and vulnerabilities than regulators and should be empowered to leverage this understanding to make informed decisions on how to best meet regulatory objectives. In addition, technology-neutral rules are key. A regulatory framework, even one that is broadly principles-based, can be undermined if it does not account for the possibility, and indeed likelihood, of innovation and new technologies. Policies with specific technology requirements are inherently reactive to changing environments and become quickly outdated.

These principles are designed to provide meaningful guidance to regulated firms about how they should structure, operate and govern virtual storage to comply with relevant regulations. Given, however, the significant differences that exist in size, organisational and legal structures of regulated firms, as well as the nature and scope of business activities conducted by them, there exists no single set of universally applicable control techniques and procedures which will guarantee the adequacy of a firm's controls. Recognising this, these principles require a proportionate and outcome focused approach, considering the scale and sophistication of a regulated firm's business and operations, designed to ensure a

reasonable degree of assurance of these outcomes. They should therefore be capable of application irrespective of the size, resources or sophistication of a regulated firm.

We also believe that the use of virtual data storage including the cloud provides substantial benefits to industry and their customers including scalability of services on demand and cost reductions versus fixed capacity equivalents.

Virtual data storage principles

These principles only cover data required by financial services regulators to be stored by regulated firms to comply with regulatory obligations.

Virtual storage of data by regulated firms should:

Principle 1 – Data access

Allow regulators access to a historical archive of all regulatorily required data for the regulatorily required period, including but not limited to transactional data.

Principle 2 – Data availability

Allow for data – regardless of physical or virtual location onshore or offshore – to be made available to the regulator within a reasonable time and in a readable format at the request of the regulator, though subject to the usual applicable legal process. In case of a search operation, access should be given via the premises of the regulated firm located in the regulator's jurisdiction.

Principle 3 – Prohibitive jurisdiction

Prohibit storage in jurisdictions the applicable regulator blacklists for reasons of those jurisdiction's laws and regulations hampering compliance with these principles.

Principle 4 – Outsourcing

Comply with applicable outsourcing regulations.

Principle 5 – Data security

Be subject to reasonably adequate physical and cyber security measures to ensure:

a. data integrity is maintained
b. data is protected from unauthorised access
c. data can only be altered for proper purposes by authorised people with an audit trail of changes
d. data is otherwise free from damage or tampering

Principle 6 – Business continuity

Be subject to reasonably adequate business continuity and disaster recovery measures to ensure:

a. safe and secure storage and proper access to data is not disrupted
b. data can be reconstructed in the case of damage or destruction

Principle 7 – Data retention

Ensure that data can be retained and transferred without compromise of compliance of these principles in case of the end of a relationship with a third-party storage vendor.

Principle 8 – Periodic review

Be reviewed periodically to ensure reasonable assurance of compliance with applicable regulations and these principles.

Principle 9 – Relevant industry standards

Comply with relevant industry standards (for example the GFMA Financial Data Handling Principles for Banks and Non-Banks, the NIST Cybersecurity Framework, ISO 27017/18 and SOC1/2/3.

Principle 10 – Personal accountability

Clearly identify and appoint one or more employees based in the jurisdiction of the relevant financial regulator who is/are responsible for taking reasonable measures to ensure that the regulated firm complies with these principles.

Strict liability for non-compliance is rarely imposed in law for breach of such obligations where there may be factors influencing non-compliance that a regulated firm cannot reasonably control. A fairer yet proportionate approach is to expect that regulated firms take reasonable measures to ensure a degree of assurance of these outcomes.