MFSA MALTA FINANCIAL SERVICES AUTHORITY

Circular

08 March 2021

Software-as-a-Service as an Outsourcing Arrangement

From time-to-time, the Malta Financial Services Authority ("MFSA", "the Authority") receives requests for clarification from financial entities in relation to the Software-as-a-Service (SaaS) cloud model within the context of outsourcing. This Circular is being issued to provide practical guidelines in this regard.

Software-as-a-Service as a Cloud Computing Service Model

The ongoing advancements in technology and the evolving business needs of financial entities have led to an unprecedented automation of operational functions and processes. In order to meet regulatory requirements, satisfy customer demands and achieve economies of scale, financial entities across all financial sectors invest in digital tools and solutions, consequently limiting exposure to human error. Such increased use of technology has resulted in developments in software and infrastructure solutions offered to financial entities. Nowadays, in order to optimise operational performance and use the benefits of cloud-based solutions, firms often opt for Software-as-a-Service (SaaS). SaaS is the most commonly used cloud computing service model and involves the consumption of web- or internet-based applications, managed by external providers.

SaaS allows organisations to perform operational tasks, manage data, as well as meet reporting and compliance obligations without the need to develop expensive software or exercise manual input, effectively enhancing usability, and reducing costs. Moreover, SaaS solutions offer constant online and offline accessibility, and usually leverage on the benefits linked to cloud computing. Amongst different types of SaaS solutions, financial entities can utilise the tools not only to foster internal operations but also to enhance customer experience.

The European Commission Cloud Strategy, published in May 2019 as an enabler of the European Commission's Digital Strategy, defines SaaS *as "business applications that are owned, delivered and managed remotely by one or more providers. The provider delivers software based on one set of common code and data definitions that is consumed in a one-to-many model by all contracted customers at any time on a pay-for-use basis or as a subscription based on use metrics."* Within the context of the vendor–user relationship, the SaaS model allows the vendor to manage the business application/s which would otherwise have to be managed in-house.

Interestingly, the Legislative Proposal for a Regulation on Digital Operational Resilience ('DORA') of 24th September 2020 (which is still at proposal stage as at the time of writing), defines 'ICT third-party service provider' as "*an undertaking providing digital and data services, including providers of cloud computing services, software, data analytics services, data centres, but excluding providers of hardware components and undertakings authorised under Union law which provide electronic communication*

services as defined referred to in point (4) of Article 2 of Directive (EU) 2018/1972 of the European Parliament and of the Council".

Establishing whether SaaS is an Outsourcing Arrangement

Under normal circumstances, the management element of the service rendered by SaaS Third Party Providers (TPPs) to licence holders, as being described, qualifies as an outsourcing arrangement. More specifically, SaaS qualifies as an outsourcing arrangement if the service is performed on a recurrent or an ongoing basis and if the service would normally fall within the scope of functions that would or could realistically be performed by the licence holder, even if the licence holder has not performed this function in the past.

Licence holders are to assess and determine whether SaaS currently being consumed or planned to be acquired, qualifies as an outsourcing arrangement. Licence holders are to further assess and determine whether the outsourcing arrangement entails the outsourcing of a critical or important function.

Further guidance on outsourcing arrangements and assessments of whether outsourcing arrangements relate to functions that are critical or important can be found within the Guidance on Technology Arrangements ICT and Security Risk Management and Outsourcing Arrangements and European Supervisory Authority guidelines on Outsourcing Arrangements and/or Outsourcing to Cloud Service Providers.

Outsourcing Risk within in the Context of SaaS

Licence holders shall manage the relevant outsourcing risks associated with SaaS arrangements, including but not limited to risks associated with the data being processed by the SaaS TPPs. Within their risk assessments, licence holders need to, for instance, give due consideration to business continuity in case of disruptions on the part of the SaaS TPP, migration and exit strategies. SaaS TPPs should be subject to adequate due diligence both at the initial stage and on an ongoing basis. Further guidance on outsourcing risk can also be found within the above referenced guidelines.

Licence holders are reminded of their obligation to comply with any applicable Acts, Regulations, rules and sector specific guidelines pertaining to outsourcing arrangements.

Licence Holders may request further feedback or clarifications by sending an email to the Supervisory ICT Risk and Cybersecurity function within MFSA on sirc@mfsa.mt.