ESMA consultation paper on draft Guidelines on outsourcing to cloud services providers

Link to the paper: *Consultation paper on draft Guidelines on outsourcing to Cloud Services Providers*

1.- Target audience (potential stakeholders):

This paper is of interest to National Competent Authorities (NCAs) and financial market participants and, in particular, to those using cloud services provided by third parties:

- Alternative investment fund management companies and depositaries
- Undertakings for collective investment in transferable securities (UCITS) management companies and depositaries
- Central Counterparties (CCPs)
- Trade repositories
- Investment firms
- Credit institutions providing investment services
- Data reporting service providers
- Operators of trading venues
- Central securities depositaries
- Credit rating agencies
- Securitisation repositories
- Administrators of benchmarks

The paper is also of interest to cloud service providers with which the aforementioned firms contract such services.

The CNMV would appreciate it if all the above-mentioned potential stakeholders were to send a copy of their responses to the consultation to the following email address: Documentosinternacional@cnmv.es

2.- Information Note

On 3 June, ESMA published draft guidelines on outsourcing to cloud service providers.

The aim of these draft guidelines is to ensure that the risks that may arise from the provision of cloud services by financial market participants are appropriately identified and addressed. These guidelines are intended to help firms identify, address and monitor the risks that may arise from their cloud outsourcing arrangements (making the decision to outsource, selecting a cloud service provider, monitoring outsourced activities and providing for exit strategies).

ESMA identified the need to issue these guidelines following the European Commission's FinTech Action Plan. Given that the main risks associated with cloud outsourcing are similar across sectors, ESMA has considered the recent guidelines published by EBA and EIOPA.

The structure of the consultation paper is as follows:

.- Section 2 contains the background of the guidelines:

Firms are increasingly using cloud services. Although these services can offer benefits and even a reduction in costs and enhanced operational efficiency and flexibility, they raise challenges in terms of data protection and information security. Concentration risk can also arise, as a result of many firms using the same cloud service, with potential negative outcomes for financial stability.

Although the general principles regarding effective controls for outsourcing are applicable to this type of outsourcing, ESMA recognises that certain features are specific to cloud services: they tend to be more standardised and are provided to clients in a highly automated manner and at large scale.

Each firm is responsible for identifying and implementing effective ways of managing risks in relation to the use of cloud services.

.- Section 3 contains the proposed guidelines together with the questions for consultation:

Guideline 1: Governance, oversight and documentation

The outsourcing of this service must be the outcome of a strategy adopted by senior management and must not be considered as an IT matter only. Furthermore, oversight of the outsourcing of services must be based on the risk-based approach. Each firm shall maintain a register of information on all its cloud outsourcing arrangements, distinguishing between the outsourcing of critical or important functions.

The guidelines apply the principle of proportionality by differentiating the firms' obligations according to how the outsourcing affects critical or important functions, or affects other types of functions.

Guideline 2: Pre-outsourcing analysis and due diligence

Before concluding an arrangement with a cloud service provider, the firm must assess whether the arrangement concerns a critical or important function, identify all potential risks and possible supervisory limitations, as well as potential conflicts of interest. In the case of outsourcing of critical or important functions, the due diligence should include an assessment of the appropriateness of the cloud service provider. In the case of changes in the supplier or the criticality of the function concerned, the firm may reassess both the pre-outsourcing analysis and the due diligence.

Guideline 3: Contractual requirements

The rights and obligations of the firm and of the cloud service provider should be set out in a written agreement, which at least contains aspects such as applicable law,

jurisdiction, countries where the data are stored or the right for the firm to monitor the the provider's performance on a regular basis.

Guideline 4: Information security

Each firm should set information security requirements in its internal policies and procedures and within the cloud outsourcing written agreement and comply with these requirements on an ongoing basis, including to protect confidential, personal or sensitive data. In the case of outsourcing of critical or important functions, the firm should, inter alia: use encryption systems, consider the segregation of networks, consider the integration with its APIs, have business continuity and disaster recovery plans in place and know its data storage and data processing location.

Guideline 5: Exit strategies

In the case of critical functions, firms should ensure that they are able to exit the cloud outsourcing arrangement without any detriment to their compliance with the applicable legal requirements, as well as the confidentiality, integrity and availability of their data, and without undue disruption to their activities.

For this purpose, firms should define the objectives of the exit strategy and the trigger events that could activate the exit strategy.

Guideline 6: Access and audit rights

Firms should ensure that the agreement concluded with the third-party provider of cloud services does not limit the firms' effective exercise of the access and audit rights of the services. Firms should assess whether the internal and external audits are appropriate and sufficient to comply with their obligations.

Guideline 7: Sub-outsourcing

If sub-outsourcing of critical or important functions is permitted, the terms and conditions agreed between the provider and the sub-outsourcer shall form part of the written agreement between the firm and the provider. Firms should ensure that the provider appropriately oversees the sub-outsourcer.

Guideline 8: Written notification to competent authorities

If a firm decides to outsource critical or important functions, it must notify its competent authority. The notification shall include, among others, a description of the outsourced function, the reasons why the outsourced function is considered critical, the details of the supplier, the governing law and the choice of jurisdiction, and the cloud deployment model.

Guideline 9: Supervision of cloud outsourcing arrangements

Competent authorities should assess the risks arising from the cloud outsourcing arrangements as part of their supervisory activities. In particular, this assessment should focus on the arrangements that relate to the outsourcing of critical or important functions. Competent authorities should be able to perform an effective supervision, in particular when the service provider is located outside the EU.

Competent authorities should assess on a risk-based approach whether firms have in place the governance, resources and operational processes required to outsource this service and to identify the relevant risks. Where concentration risks are identified, competent authorities should monitor their potential impact on other firms and the stability of the financial market.

.- *Appendix 1* contains all the questions set out in the consultation paper. *Appendix 2* includes a preliminary cost/benefit analysis.

ESMA shall consider the responses it receives to this consultation paper in Q32020 and expects to publish a final report in Q42020/Q12021.

These guidelines apply from 30 June 2021 to all cloud outsourcing arrangements concluded, renewed or amended on or after this date. Firms should review and amend accordingly existing cloud outsourcing arrangements with a view to ensuring that they take into account these guidelines by 31 December 2022. Where the review of cloud outsourcing arrangements of critical or important functions is not finalised by 31 December 2022, firms should inform their competent authority of this fact, including the measures planned to complete the review or the possible exit strategy.

3.- Submission of comments

The deadline for submitting comments is **1 September 2020**.

Respondents may send their comments through the online response form available at the following link: https://ec.europa.eu/info/publications/finance-consultations-2020-non-financial-reporting-directive_en

Likewise, as indicated above, the CNMV would also appreciate it if stakeholders could send a copy of their responses to the consultation to the following email address: Documentosinternacional@cnmv.es

CNMV
Dirección de Asuntos Internacionales
c/ Edison 4
28006 Madrid