|  |
| --- |
| Response Form to the Consultation Paper |
| Guidelines on Outsourcing to Cloud Service Providers |

**Responding to this paper**

ESMA invites comments on all matters in this consultation paper on guidelines on outsourcing to cloud service providers and in particular on the specific questions summarised in Appendix I. Comments are most helpful if they:

* respond to the question stated;
* indicate the specific question to which the comment relates;
* contain a clear rationale; and
* describe any alternatives ESMA should consider.

ESMA will consider all comments received by **01 September 2020.**

All contributions should be submitted online at [www.esma.europa.eu](http://www.esma.europa.eu) under the heading ‘Your input - Consultations’.

**Instructions**

In order to facilitate analysis of responses to the Consultation Paper, respondents are requested to follow the below steps when preparing and submitting their response:

1. Insert your responses to the questions in the Consultation Paper in the present response form.
2. Please do not remove tags of the type <ESMA\_QUESTION\_COGL\_1>. Your response to each question has to be framed by the two tags corresponding to the question.
3. If you do not wish to respond to a given question, please do not delete it but simply leave the text “TYPE YOUR TEXT HERE” between the tags.
4. When you have drafted your response, name your response form according to the following convention: ESMA\_COGL\_nameofrespondent\_RESPONSEFORM. For example, for a respondent named ABCD, the response form would be entitled ESMA\_COGL\_ABCD\_RESPONSEFORM.
5. Upload the form containing your responses, in Word format, to ESMA’s website ([www.esma.europa.eu](http://www.esma.europa.eu) under the heading “Your input – Open consultations” 🡪 “Consultation on Outsourcing to Cloud Service Providers”).

**Publication of responses**

All contributions received will be published following the close of the consultation, unless you request otherwise. A standard confidentiality statement in an email message will not be treated as a request for non-disclosure. A confidential response may be requested from us in accordance with ESMA’s rules on access to documents. We may consult you if we receive such a request. Any decision we make not to disclose the response is reviewable by ESMA’s Board of Appeal and the European Ombudsman.

**Data protection**

Information on data protection can be found at [www.esma.europa.eu](http://www.esma.europa.eu) under the heading [Legal Notice](http://www.esma.europa.eu/legal-notice).

**Who should read this paper**

This paper is primarily of interest to national competent authorities and financial market participants. In particular, this paper is of interest to alternative investment fund managers, depositaries of alternative investment funds, undertakings for collective investment in transferable securities (UCITS) management companies, depositaries of UCITS, central counterparties, trade repositories, investment firms and credit institutions which carry out investment services and activities, data reporting services providers, market operators of trading venues, central securities depositories, credit rating agencies, securitisation repositories and administrators of benchmarks (“firms”), which use cloud services provided by third parties. This paper is also important for cloud service providers, because the draft guidelines seek to ensure that the risks that may arise for firms from the use of cloud services are properly addressed.

**General information about respondent**

|  |  |
| --- | --- |
| Name of the company / organisation | Amazon Web Services EMEA SARL |
| Activity | Non-financial counterparty |
| Are you representing an association? |  |
| Country/Region | Europe |

**Introduction**

***Please make your introductory comments below, if any***

<ESMA\_COMMENT\_COGL\_1>

AWS welcomes the opportunity to provide comments on the ESMA consultation paper on draft Guidelines on Outsourcing to Cloud Service Providers (“ESMA Guidelines”). We acknowledge the ongoing efforts by the three European Supervisory Authorities (ESAs) in terms of developing a consistent regulatory approach for EU financial organisations looking to move workloads to the cloud.

In addition to AWS responses to the Questions for Consultation in the online questionnaire, we have also included suggested wording that reflect the issues raised in the responses. Further, we would like to highlight the need for clarity on the applicability of the ESMA Guidelines for non-EU central counterparties (CCPs) and non-EU benchmarks administrators. Specifically, the current wording in paragraph 15 of the ESMA Guidelines creates ambiguity as to whether and to what extent the ESMA Guidelines will apply to these entities. Given the potential extraterritorial impact, and in order to avoid duplicative and/or conflictive regimes, we urge ESMA to clarify that non-EU CCPs and non-EU benchmarks administrators are not required to implement the ESMA Guidelines. We would also suggest ESMA considers the ongoing work by the International Organization of Securities Commissions (IOSCO) on the Principles on Outsourcing aiming to ensure international coordination.

Further, we strongly believe the ESMA Guidelines should align to those already published by the European Banking Authority (EBA) and the European Insurance and Occupational Pensions Authority (EIOPA) in order to avoid regulatory and supervisory fragmentation. We believe the establishment of a coherent and fair regulatory framework for the use of cloud services is critical in order to support the long term competitiveness of the EU financial services sector by enabling its digitalisation.

AWS remains committed to supporting European financial services organizations wishing to adopt cloud services in the safest of environments, ensuring their security and resiliency. We thank ESMA for the opportunity to comment on the proposed ESMA Guidelines, and would appreciate the opportunity to discuss any of the comments or suggestions included in the submission at a time of your convenience.

<ESMA\_COMMENT\_COGL\_1>

**Questions**

1. : Do you agree with the suggested approach regarding a firm’s governance and oversight in relation to its cloud outsourcing arrangements? Please explain.

<ESMA\_QUESTION\_COGL\_1>

TYPE YOUR TEXT HERE

<ESMA\_QUESTION\_COGL\_1>

1. : Do you agree with the suggested documentation requirements? Please explain.

<ESMA\_QUESTION\_COGL\_2>

TYPE YOUR TEXT HERE

<ESMA\_QUESTION\_COGL\_2>

1. : Do you agree with the suggested approach regarding the pre-outsourcing analysis and due diligence to be undertaken by a firm on its CSP? Please explain.

<ESMA\_QUESTION\_COGL\_3>

TYPE YOUR TEXT HERE

<ESMA\_QUESTION\_COGL\_3>

1. : Do you agree with the proposed contractual requirements? Please explain.

<ESMA\_QUESTION\_COGL\_4>

TYPE YOUR TEXT HERE

<ESMA\_QUESTION\_COGL\_4>

1. : Do you agree with the suggested approach regarding information security? Please explain.

<ESMA\_QUESTION\_COGL\_5>

TYPE YOUR TEXT HERE

<ESMA\_QUESTION\_COGL\_5>

1. : Do you agree with the suggested approach regarding exit strategies? Please explain.

<ESMA\_QUESTION\_COGL\_6>

Paragraph 44 (c) does not adequately take in account the nature of the public cloud and the role of the cloud service provider in the transfer of data upon exit. AWS’s services are generally made available to firms to use on a self-service basis without any direct intervention from AWS. AWS provides services that allow firms to transfer but does not play an active or customized role in the process. AWS’s services are generally made available to firms to use on a self-service basis without any direct intervention from AWS. Therefore, we suggest that ESMA adopts the edits proposed below. The CSP’s commitment to “*support the orderly transfer of the outsourced function*” would be consistent with the requirements under paragraph 99 of the EBA Guidelines.

Further, the requirement for firms to ensure “*that any data removed or transferred is securely deleted from the systems of the CSP and, where applicable, of any sub-outsourcer by, for example, requesting a written confirmation by the CSP*” in case of outsourcing of critical or important functions needs to be interpreted in the context of the public cloud (which relies on a standardised self-service model) as firms retain complete control over how and when to delete its data. Specifically in relation to AWS:

i) AWS services are designed to give customers the tools and ability to manage their own content on a self-service basis, including the deletion of that content. AWS customers have the freedom to decide what content to upload on to AWS, when, where, whether to delete it and how. AWS does not control or process customer content in any meaningful way. As the AWS services are self-service, they merely respond automatically to the customer's instructions, which the customer inputs via the AWS Management Console or the APIs (Application Programming Interfaces).

ii) AWS does not manage the deletion functionality on the customer's behalf. If the customer wants to delete customer content (whether in the course of using the AWS services or when it stops using the AWS services), the customer can use the AWS Management Console or the APIs to instruct the AWS services to delete the instances of customer content which the customer wants to delete. In addition, customers are able to securely delete their content by, for example, encrypting their data and then destroying their encryption keys.

Further, the EBA Guidelines emphasise the transfer and continuity of the service (paragraph 99 of the EBA Guidelines), leaving the deletion of the data within the control of the firm. The GDPR (at article 28(3)(g)) also makes it clear that it is at the choice of the controller (the undertaking) to delete its data.

Given the above, we suggest ESMA considers the following revised text:

44. c) ensure that the cloud outsourcing written agreement includes an obligation for the CSP to **support the** orderly transfer **of** the outsourced function and all the related data from the CSP and any sub-outsourcer to another CSP indicated by the firm or directly to the firm in case the firm activates the exit strategy;

ensure that any data removed or transferred is securely deleted from the systems of the CSP and, where applicable, of any sub-outsourcer (for example, by requesting a written confirmation by the CSP)

<ESMA\_QUESTION\_COGL\_6>

1. : Do you agree with the suggested approach regarding access and audit rights? Please explain.

<ESMA\_QUESTION\_COGL\_7>

We understand that paragraph 52 would be only applicable to the outsourcing of critical or important functions, and recommend to introduce further clarification on this. This will avoid confusion over the applicability of paragraph 52 to the outsourcing of both critical and non-critical functions. Not specifying the applicability of paragraph 52 to the outsourcing of critical or important functions would constitute a highly problematic and material divergence from both the EBA Guidelines and the EIOPA Guidelines (see paragraph 92 of the EBA Guidelines and paragraph 46 of the EIOPA Guidelines). For the outsourcing of critical or important functions, firms should assess whether those third-parties certifications and internal or external reports are adequate and sufficient to comply with their regulatory obligations and should make use of the third-parties certifications and reports only if certain conditions are complied with.

We urge ESMA to consider aligning the ESMA Guidelines with those published by the EBA (paragraphs 92) and EIOPA (paragraphs 46), to ensure consistency and reduce the risk of regulatory fragmentation in this area. Thus, we suggest ESMA considers the following revised text:

52. In any case, **in relation to the outsourcing of critical or important functions** the firm should assess whether the third-party certifications and external or internal audit reports are adequate and sufficient to comply with its regulatory obligations and, should not solely rely on these certification and reports over time

<ESMA\_QUESTION\_COGL\_7>

1. : Do you agree with the suggested approach regarding sub-outsourcing? Please explain.

<ESMA\_QUESTION\_COGL\_8>

The definition of “sub-outsourcing” as included in Paragraph 3.2 (“Definitions; Sub-outsourcing”) is not consistent with the approach on sub-outsourcing in both the EBA Guidelines and the EIOPA Guidelines. In particular, the phrase “*or a part of that function*” in the definition is ambiguous. For example, this phrase could be interpreted to capture an insignificant portion of the outsourced function, such as day-to-day service contracts that a service provider has in place with third parties (e.g., agreements with third parties for facilities maintenance).

We strongly suggest that the ESMA Guidelines align with the EBA Guidelines and/or with the EIOPA Guidelines, as far as possible, to create consistency and reduce the risk of regulatory fragmentation in this area. In this context, we suggest ESMA considers the following revised text:

55. If sub-outsourcing of critical or important functions ~~(or a part thereof)~~ is permitted, the cloud outsourcing written agreement between the firm and the CSP should:…

<ESMA\_QUESTION\_COGL\_8>

1. : Do you agree with the suggested notification requirements to competent authorities? Please explain.

<ESMA\_QUESTION\_COGL\_9>

TYPE YOUR TEXT HERE

<ESMA\_QUESTION\_COGL\_9>

1. : Do you agree with the suggested approach regarding the supervision of cloud outsourcing arrangements by competent authorities? Please explain.

<ESMA\_QUESTION\_COGL\_10>

TYPE YOUR TEXT HERE

<ESMA\_QUESTION\_COGL\_10>

1. : Do you have any further comment or suggestion on the draft guidelines? Please explain.

<ESMA\_QUESTION\_COGL\_11>

1. Definition of Sub-Outsourcing.

Please refer to answer to Question 8 above.

We suggest ESMA considers the following revised text:

**Definitions**

*“sub-outsourcing” means a situation where the CSP further transfers the outsourced function ~~(or a part of that function)~~ to another service provider under an outsourcing arrangement*

*2. Scope (Paragraph 15)*

As mentioned in AWS introductory comments, Paragraph 15 creates ambiguity as to whether and to what extent the ESMA Guidelines will apply to non-EU CCPs and non-EU benchmark administrators. Given the potential extraterritorial impact, and in order to avoid duplicative and/or conflictive regimes, we urge ESMA to clarify that non-EU CCPs and non-EU benchmarks administrators are not required to implement the ESMA Guidelines.

Therefore, we suggest that ESMA deletes paragraph 15:

~~15. ESMA will also take these guidelines into account when assessing the extent to which (i) compliance with the relevant EMIR requirements by a Tier 2 third-country CCP is satisfied by its compliance with comparable requirements in the third country pursuant to Article 25(2b)(a) of EMIR, and (ii) application of the relevant IOSCO principles by a third-country administrator of benchmarks seeking recognition is equivalent to compliance with the applicable requirements in the Benchmarks Regulation pursuant to Article 32(2) of the Benchmarks Regulation.~~

<ESMA\_QUESTION\_COGL\_11>

1. : What level of resources (financial and other) would be required to implement and comply with the guidelines and for which related cost (please distinguish between one off and ongoing costs)? When responding to this question, please provide information on the size, internal set-up and the nature, scale and complexity of the activities of your organization, where relevant.

<ESMA\_QUESTION\_COGL\_12>

TYPE YOUR TEXT HERE

<ESMA\_QUESTION\_COGL\_12>