|  |
| --- |
| 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 | Dutch Fund and Asset Management Association |
| Activity | Investment Services |
| Are you representing an association? |[x]
| Country/Region | Netherlands |

**Introduction**

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

<ESMA\_COMMENT\_COGL\_1>

The Dutch Fund and Asset Management Association (DUFAS) welcomes the opportunity to respond to ESMA’s consultation.

DUFAS promotes the collective interests of asset managers, investment firms and custodians, operating on and from the Dutch market place – both Dutch and foreign parties. DUFAS has a commercial focus, aimed at creating both institutional and retail business opportunities for its members. Central to this is the promotion of an optimal business climate for asset management in the Netherlands. A level playing field for free supply of investment products and asset management services within the European Union and a broadening of the market for investment products are key. Dufas represents over 95% of the Dutch asset management market, both retail and institutional business. Next to independent asset management firms, self-managed (real estate) funds and custodians, Dufas membership is comprised of asset management firms that are linked to banking, insurance and pension funds. For more information, see: www.dufas.nl

<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>

.

<ESMA\_QUESTION\_COGL\_1>

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

<ESMA\_QUESTION\_COGL\_2>

We do not see the added value of an (extra) register in this context. This results in administrative burdens in the form of internal controls. In case of additional supervision requirements, these should be integrated into the existing frameworks, instead of creating separate frameworks, processes and registers specific to this type of outsourcing agreement.

Making a distinction between outsourcing to the cloud or "traditional" outsourcing agreements in the field of governance is hardly justified. A separate cloud outsourcing regime encourages the development of different interpretations and increases complexity for both the outsourcer and the CSP

The level of detail required for the register poses an additional administrative burden, which in our view is disproportionate. First, most requirements to be registered will already be included in the required risk assessment and/or notification to the authority. Second, the biggest risks generally relate to the operations rather than a legal dispute which may be under a foreign law. Being required to register for administrative purposes takes the focus off the operational risks. We believe that it is possible to remain in control when the register is without the information in sub g) to sub m).

Keeping such a register results in an increase in costs that cannot be justified by the objective of the regulator.

<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>

The due diligence is an adequate mean to assess the risks provided by outsourcing to a CSP. However the requirement 33 a) sub vi. to assess the legal system of the countries where the outsourced services may be provided is beyond what is reasonable and necessary. Generally the contract with a CSP is already under a different legal system than where the firm is located. Furthermore, the agreed law and jurisdiction are different form where the services are actually provided. Requiring a firm to assess the legal system of the places where the outsourced services may be provided including things like insolvency law goes beyond what can reasonably be expected when assessing risks that come with outsourcing. Complying with this requirement will lead to firms having to obtain external legal advice, while the contract itself is under a different legal system. We consider this requirement to be disproportionate.

-Further, we doubt the added value of periodic repetition of due diligence at a different time than when there is a material change in the nature, scale or complexity of the outsourcing agreement.

<ESMA\_QUESTION\_COGL\_3>

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

<ESMA\_QUESTION\_COGL\_4>

To a limited extent, company visits provide a realistic picture of the performance of the CSP and the way in which an attempt is made to be compliant or to provide an adequate level of security. The use of certification as a basis for correct business operations can provide support to relatively small outsourcing parties (EBA Guidelines on outsourcing, paragraaf 92-93).

<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>

In the requirement for the exit strategy, the high-level exit plan and the actual exit seem to be intertwined. Things such as defining the business impact, defining successful transition criteria and assigning roles and responsibilities are generally only necessary and possible when the actual exit takes place. As long as it has been agreed with a CSP that they will support the exit, will not decrease the level of service during the exit and return the data, the exit strategy will generally only become relevant – and should therefore only be required – when an exit actually takes place. The requirements which are currently included under ‘exit strategy’ therefore seems less strategic rather than practical steps when the exit takes place

<ESMA\_QUESTION\_COGL\_6>

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

<ESMA\_QUESTION\_COGL\_7>

In this case it is not clear what exactly is expected of financial institutions in addition to obtaining the aforementioned external and / or internal audit reports.

Cloud service providers may not easily provide a Right-to-audit. It is desirable to place more emphasis on the scope of CSP certifications and to present specific use cases for which the regulator requires (additional) substantiation.

It is superfluous/redundant to check whether these third-party certifications comply with legislation and regulations . It should be the other way around: a legislator should rule that CSP provide specific certificates at the request of a financial institution. No certificate: no possibility to offer services to a financial party.

<ESMA\_QUESTION\_COGL\_7>

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

<ESMA\_QUESTION\_COGL\_8>

As long as ESMA considers any provision of services in the chain to be outsourcing, the requirement 55 e) will pose a practical issue. CSP’s are not likely to provide all customers a right for specific approval of subcontractors. Furthermore, the right to object is generally only a paper right as customers are notified only through a specific website and can then object within a few weeks, with the consequence that customer will need to terminate the service. The protection that ESMA intends to provide with this requirement will in our view only provide protection on paper.

<ESMA\_QUESTION\_COGL\_8>

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

<ESMA\_QUESTION\_COGL\_9>

Given that a notification to the authorities will be made prior to the outsourcing of critical or important outsourced functions, the requirements of point 58 sub h) and i) seem obsolete. The question is how relevant knowing the dates for assessment of outsourcing and the risk assessment are for the authorities, as these are relevant for the internal processes.

-Regarding point 58 sub j) specifically: it is the firm as such that is responsible and accountable for an outsourcing. We therefore believe notifying to the authorities the name of an individual that has taken the decision to outsource is questionable from a GDPR perspective. We consider that there is no legal ground for this requirement to become legal obligation on which ground the provision of such name can be justified nor is it necessary information, as the firm as such remains the responsible entity anyways, therefore probably cannot be provided on the ground of legitimate interest either.

<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>

Given that only outsourcing of critical or important services or functions need to be notified to the authorities, how will supervision by the authorities as envisioned in these guidelines of outsourcing for the non-critical and not important services and functions take place? This emphasizes our view that these guidelines should be limited to outsourcing of critical or important services or functions.

<ESMA\_QUESTION\_COGL\_10>

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

<ESMA\_QUESTION\_COGL\_11>

-Given that ESMA considers any provision of services or functions in the cloud by a third party outsourcing, rather than merely the critical or important services or functions, these guidelines and the supervision of authorities should be limited to the critical or important services or functions. If a service or function is not critical or important, then outsourcing this service or function will have no or merely small impact on the firm. We believe therefore that outsourcing of non-critical or not important services or functions should not be considered regulated outsourcing in the first place and therefore be taken out of these guidelines.

Cloud-outsoucing should not be treated in a different way than outsourcing of critical and important core activities of the financial firm. Specific legislation of cloud-outsourcing will enhance the complexity of this specific topic.

<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>

Generally, the risk assessment and inclusion of contractual requirements specifically for regulated outsourcing which already takes place for what we consider outsourcing requires a lot of work from various business units (operations, IT architecture, security, procurement, legal, compliance). We believe this can currently already be translated into one-off fulltime work of 2 FTE for about 2 – 3 weeks for the critical and important services and functions.

Additional administrative tasks required by these guidelines (on top of the already existing administrative tasks), various business units will need to make available more resources (operations, compliance, security). We foresee quite some additional work, however cannot estimate these yet

<ESMA\_QUESTION\_COGL\_12>