|  |
| --- |
| 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. Please clearly and prominently indicate in your submission any part you do not wish to be publicly disclosed. 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 | Pinset Masons |
| Activity | Audit/Legal/Individual |
| Are you representing an association? |[ ]
| Country/Region | International |

**Introduction**

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

<ESMA\_COMMENT\_COGL\_1>

 If you would like any more information about Pinsent Masons or the information contained in this guide, please contact our specialist team members:

**Luke Scanlon**

Head of Fintech Propositions

Legal Director

T: +44 20 7490 6597

M: +44 7887 815 950

E: luke.scanlon@pinsentmasons.com

**Ruth Maria Bousonville**

Legal Director

Risk Advisory Services

T: +49 69 506026 017

M: +49 173 248 55 34

E: ruthmaria.bousonville@pinsentmasons.com

**About Pinsent Masons**

Pinsent Masons is a full-service international commercial law firm with more than 400 partners and 1,500 lawyers in 26 offices across the world.

We concentrate on five core sectors – two of which are financial services and technology. Our sector led approach enables us to work more closely with our clients to understand their needs, objectives and to align our strategies. This helps us to give pragmatic, commercial advice and develop innovative propositions. We share with our clients the deep collective insight, local knowledge, international experience and networks of our people working in a sector.

At Pinsent Masons, we help our clients satisfy their customers' expectations. Whether a global bank, a leading insurer, wealth provider, emerging fintech or technology provider, we can help you navigate the ever-changing legal and regulatory frameworks and technology and data risks that may otherwise stand in your way.

As a leading international law firm, we also advise on all aspects of the technology sourcing lifecycle including on first generation outsourcings and the re-structuring of existing arrangements to achieve desired business outcomes. This gives us the insight to understand how sourcing contracts work in practice, and has allowed us to develop a keen eye for the kind of contractual issues that can arise.

<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>

 *Issue 1 – the definition of a cloud service provider*

We suggest that ESMA narrow the definition of a cloud service provider (CSP).

We appreciate that ESMA has broadened the definition of a CSP to address risks that can arise when a CSP is in the background of an outsourcing arrangement and not the party directly engaged by the regulated entity. However, ESMA's approach is inconsistent with that taken by of the European Banking Authority (EBA) and the European Insurance and Occupational Pensions Authority (EIOPA) in their respective outsourcing and cloud guidelines.

To further objectives of harmonisation and consistency, we suggest that ESMA follow the approach taken by the EBA and EIOPA. Our understanding gained from the experiences of our clients is that the negative impact of inconsistent guidelines between the European Supervisory Authorities (ESAs) creates significant additional cost and implementation risks which outweigh any benefits to be gained by introducing inconsistent definitions.

Alternatively, if ESMA does not agree with our assessment of the potential additional risks created by inconsistent definitions, we suggest that ESMA narrow the definition of a CSP in order to remove the concept of a third party "relying on a CSP".

We are concerned that the new concept of "relying on a CSP" will introduce a high level of uncertainty as the guidelines do not give any criteria to assist in determining the extent to which a third party would need to "rely" on a CSP for the arrangement to be considered within the scope of the guidelines. A more consistent approach with the underlying legislative framework would be closely relate the definition of a CSP to that of outsourcing and sub-outsourcing by limiting it to cloud providers to whom outsourcing and sub-outsourcing providers "further transfer" their material obligations under contracts with regulated entities.

<ESMA\_QUESTION\_COGL\_1>

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

<ESMA\_QUESTION\_COGL\_2>

 *Issue 2 – the cloud register and data processing locations*

We suggest that the requirement to keep records of data *processing* locations be removed.

Paragraph 29(h) requires regulated entities to maintain on their registers for cloud arrangements details of "the specific nature of the data to be held and the locations (namely countries) where such data may be stored and processed."

It is disproportionate to the risk to require regulated entities to obtain details of all *processing locations* of data in addition to *storage locations* in a cloud context. Strictly interpreted, this guideline may require regulated entities to list out all jurisdictions through which data merely passes in transit across the internet.

We are aware of no evidence that suggests that naming locations through which data merely transits will reduce any risk of data being unlawfully disclosed or intercepted where those locations are required *in addition* to the locations where data will be stored when at rest.

<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>

*Issue 3 – personal data processing requirements "over and above" GDPR*

We suggest that ESMA clarify that it is not limiting the choices which regulated entities may have under data protection laws.

ESMA sets out various risk assessment steps for regulated entities to take in relation to data. In practice, the details of similar guidelines which the EBA has issued have created uncertainties around whether or not the ESAs intend to impose requirements which relate to data that are more stringent than those imposed by the General Data Protection Regulation (GDPR) and data protection supervisory authorities.

We suggest that ESMA clarify that it does not intend to impose any rules relating to the processing of data which are in excess of those required under GDPR and by data protection supervisory authorities. If a regulated entity has taken all necessary steps to comply with the data protection regulatory framework, the ESMA guidelines should not be viewed as further restricting transfers of data where the transfer would otherwise be permissible but for the ESMA guideline.

A clear statement that it is not the intention of ESMA to restrict the compliance options regulated entities have at their disposal under the data protection regulatory framework will lead to more certainty and a reduction of cost for regulated entities in addressing data protection issues.

*Issue 4 – concentration risk across the sector*

We suggest that the requirement for regulated entities to monitor concentration risk across the sector should be deleted.

Regulated entities are asked in paragraph 33(a)(vii) to assess all relevant risks arising from "possible concentration within the sector, caused by multiple firms making use of the same CSP or a small group of CSPs" in addition to concentration risks they may individually face as regulated entities. Our view is that this guidance should be deleted as practically it is very difficult to achieve and may result in regulated entities making unfavourable decisions due to limitations they may have in accessing relevant data.

Regulated entities will not have access to commercially sensitive information held by CSPs in order to determine with any level of accuracy the extent to which possible concentrations are occurring within the sector. They will therefore be relying on data provided by third parties or that is publicly available, either of which may be inaccurate or give an accurate view of the overall picture. We do not think that it is advisable for regulated entities to be making key risk decisions on such as uncertain basis, and that concerns around concentration risk across the sector should be addressed by regulators rather than regulated entities.

We therefore recommend that the words "as well as possible concentration within the sector, caused by multiple firms making use of the same CSP or a small group of CSPs" be deleted.

*Issue 5 – business continuity and disaster recovery plans*

We suggest that ESMA reframe the focus to be on *suitable* business continuity plans rather than reviewing the *details of all plans*.

Paragraph 34(c) suggests that regulated entities as part of due diligence view the business continuity and disaster recovery plans of CSPs. We question whether this would always be necessary if taking a risk-based approach, and suggest that the ESMA guidelines align with the EBA approach which sets out that the outsourcing provider should give an assurance that it has suitable business continuity plans proportionate to the risk of the services provided but does not require the plans themselves to be reviewed.

For security reasons, CSPs may be justified in not providing all details of the actions they would take in the event of disruption or disaster to a customer. If the CSP has assured the customer that it has met a specific standard, list of criteria or other means of assessing suitability, this may be preferable to compelling the CSP to provide all details of its plans.

<ESMA\_QUESTION\_COGL\_3>

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

<ESMA\_QUESTION\_COGL\_4>

 *Issue 6 – data processing locations in addition to storage locations*

Paragraph 41(f) sets out that "In case of outsourcing of critical or important functions, the written agreement should set out at least ... the location(s) (namely countries) where relevant data will be stored and processed (location of data centres), and the conditions to be met, including a requirement to notify the firm if the CSP proposes to change the location(s)."

See our earlier comments in relation to issue 2.

We suggest that this paragraph be amended so that it reads: "In case of outsourcing of critical or important functions, the written agreement should set out at least ... the location(s) (namely countries) where relevant data will be stored ~~and processed~~ (location of data centres), and the conditions to be met, including a requirement to notify the firm if the CSP proposes to change the location(s)."

*Issue 7 – the concept of 'data ownership' is an inaccurate one*

We recommend that the ESMA guidelines do not refer to 'data ownership'.

Paragraph 41(o) provides that "In case of outsourcing of critical or important functions, the written agreement should set out at least ... provisions to ensure that the data owned by the firm can be recovered by the firm as needed, having regard to Guideline 5."

Under the laws of many jurisdictions, it is factually inaccurate to describe data as subject to "ownership". The regulated entity and its customers will have rights over data such as those set out in copyright, database right and data protection laws. However, under most legal frameworks the entity and its customer will not be considered the 'owner' of the data as that term is used in a legal sense but the controller or possessor of it.

It would be preferable for the guidelines to refer to data that the CSP processes on behalf of the firm rather than "data owned by the firm".

<ESMA\_QUESTION\_COGL\_4>

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

<ESMA\_QUESTION\_COGL\_5>

 *Issue 8 – maintaining flexibility in how best to address information security risks*

We think that ESMA should remove references to specific information security practices.

ESMA has outlined various steps that a regulated entity can take in setting its information security requirements. We are concerned that ESMA has, on the one hand, included more detailed statements than the other ESAs have included in guidelines, but on the other, not gone far enough in order to provide regulated entities with a comprehensive list to follow.

Accordingly, we think that the better approach would be for ESMA to remove the specific references to information security practices that have been included in the draft to avoid the conclusion that these practices are more important than the many other information security practices that have not been included. Alignment with the other ESAs will create more certainty in how regulated entities and CSPs can address security concerns.

The references that are unique to the ESMA guidelines which we suggested should be deleted are:

* "ensuring that strong authentication mechanisms (for example two factor authentication";
* "appropriate levels of segregating networks (for example tenant isolation in the shared environment of the cloud, operational separation as regards the web, application logic, operating system, network, Data Base Management System (DBMS) and storage layers) and processing environments (for example test, User Acceptance Testing, development, production)"; and
* "establishing and maintaining information security policies and procedures for APIs across multiple system interfaces, jurisdictions, and business functions to prevent unauthorised disclosure, modification or destruction of data."

Deleting these references avoids the unintended consequence of technical security teams within regulated entities and CSPs building solutions to meet the specific words of regulatory guidance even if to do so would not be best practice from a security risk perspective.

We also suggest that ESMA use clearer but broader language to ensure that regulated entities take appropriate steps to ensure that their information security practices meet legal requirements.

<ESMA\_QUESTION\_COGL\_5>

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

<ESMA\_QUESTION\_COGL\_6>

*Issue 9 – clarifying expectations when carrying out "sufficient" exit planning tests*

We think that ESMA should adopt the clarifications used by the other ESAs to explain the requirements for an exit plan test to be '"sufficient".

Paragraph 44(d) provides that "In case of outsourcing of critical or important functions, a firm should ensure that it is able to exit cloud outsourcing arrangements without undue disruption to its business activities and services to its clients, and without any detriment to its compliance with the applicable legal requirements, as well as the confidentiality, integrity and availability of its data. To achieve this, a firm should ... develop and implement exit plans that are comprehensive, documented and sufficiently tested. These plans should be updated as needed, including in case of changes in the outsourced function. "

This paragraph does not define what a "sufficient test" of an exit plan may involve. We had previously suggested to EIOPA following its draft guidelines that it bring it into line with the EBA's approach and set out some criteria for a "sufficient test". EIOPA in its final guidelines adopted the approach taken by the EBA.

The EBA sets out that a sufficient test can involve "carrying out an analysis of the potential costs, impacts, resources and timing implications of transferring an outsourced service to an alternative provider." This avoids any suggestion that actual resources would need to transfer from one CSP to another which would not be viable in many circumstances.

<ESMA\_QUESTION\_COGL\_6>

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

<ESMA\_QUESTION\_COGL\_7>

*Issue 10 – expanding the scope of third party certifications*

We think that ESMA should not ask regulated entities to obtain a right to expand the scope of third party certifications.

Paragraph 51(f) provides that "In case of outsourcing of critical or important functions, a firm should make use of the third-party certifications and external or internal audit reports ... only if it .... [it] "has the contractual right to request the expansion of the scope of the certifications or audit reports to other relevant systems and controls of the CSP."

We can see the value in obtaining a right to expand the scope of an audit report but not of a third party certification. Third party certifications by their nature need to be set to specific standards and therefore cannot be changed to accommodate the bespoke needs of individual organisations. The benefit of the certification is that the high (though generalised) standard maintained is suitable and reached by the CSP.

It would be inconsistent to suggest that on the one hand both parties can gain comfort from a certification that is performed against accepted international standards, and on the other, require that those certifications move away from the set international standard to meet the needs of each customer of the CSP which relies on the certification.

We suggest that paragraph 51(f) be amended as follows: "In case of outsourcing of critical or important functions, a firm should make use of ~~the third-party certifications and~~ external or internal audit reports ... only if it .... [it] "has the contractual right to request the expansion of the scope of the ~~certifications or~~ audit reports to other relevant systems and controls of the CSP."

<ESMA\_QUESTION\_COGL\_7>

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

<ESMA\_QUESTION\_COGL\_8>

*Issue 11 – uncertainty as to when the obligation to notify of changes to sub-outsourcing applies*

We suggest that ESMA clarify the circumstances in which the CSP must notify the customer of a material change in its sub-outsourcing arrangements.

Paragraph 55(d) sets out that "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 … include an obligation for the CSP to notify the firm of any planned sub-outsourcing, or material changes thereof, in particular where that might affect the ability of the CSP to meet its obligations under the cloud outsourcing arrangement with the firm."

The words "in particular" create uncertainty as to the circumstances for which the regulated entity is required to retain a right to be notified of a change in sub-outsourcers or material change to a sub-outsourcing arrangement. It is unclear whether the CSP should notify the regulated entity for:

* *any and all* planned sub-outsourcings or material changes to sub-outsourcings; or
* *only* planned sub-outsourcings and material changes to sub-outsourcings where the planned sub-outsourcing or material change *might affect the ability of the CSP to meet its obligations* under the cloud outsourcing arrangement with the firm; or
* in *other circumstances* – a middle third category of circumstances that are additional to those which might affect the ability of the CSP to meet its obligations under the cloud outsourcing arrangement but fall short of all new sub-outsourcing arrangements and material changes.

We suggest that ESMA avoid these uncertainties by amending paragraph 55(d) so that it reads ... "include an obligation for the CSP to notify the firm of any planned sub-outsourcing, or material changes thereof, ~~in particular~~ where that planned sub-outsourcing or material change might affect the ability of the CSP to meet its obligations under the cloud outsourcing arrangement with the firm."

<ESMA\_QUESTION\_COGL\_8>

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

<ESMA\_QUESTION\_COGL\_9>

We agree with these requirements subject to our comments in relation to paragraph 57(e) and (f) - see issue 2 above.

<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>

Yes.

<ESMA\_QUESTION\_COGL\_10>

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

<ESMA\_QUESTION\_COGL\_11>

No.

<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>

No comment.

<ESMA\_QUESTION\_COGL\_12>