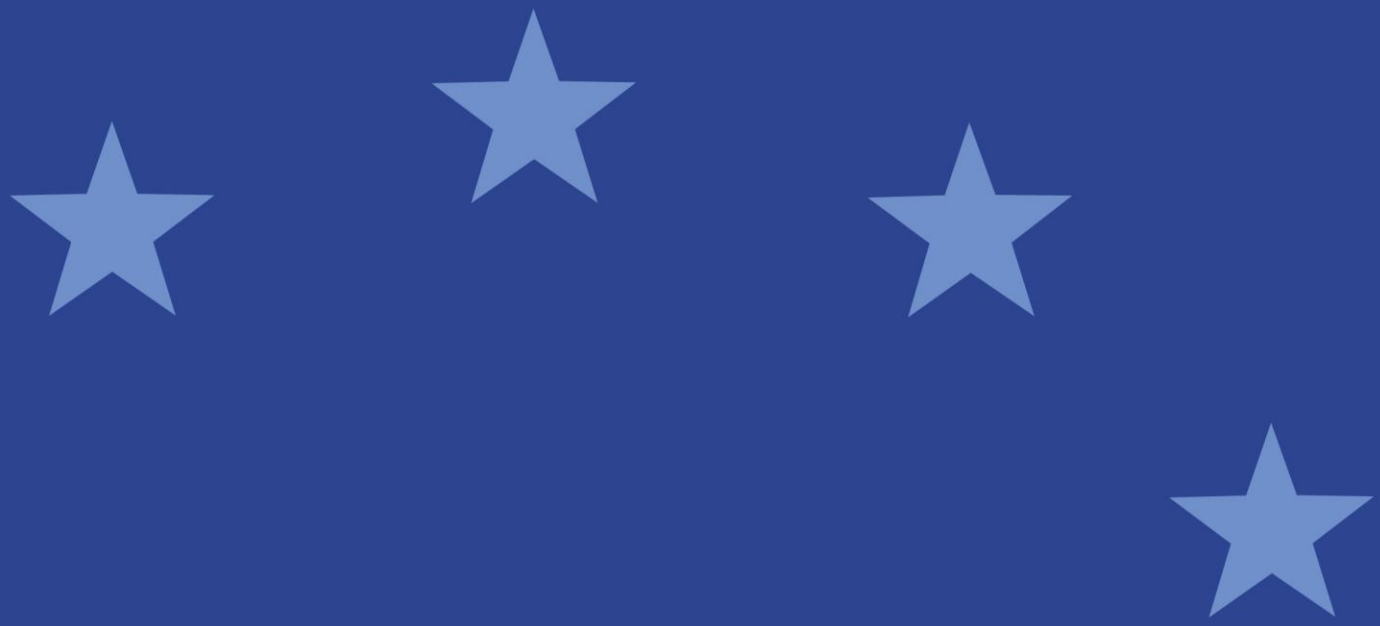
esma European Securities and Markets Authority

Response Form to the Consultation Paper

Guidelines on Outsourcing to Cloud Service Providers



03 June 2020 ESMA-XX-XXX

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 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 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 under the heading 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	Deutsche Börse Group
Activity	Regulated markets/Exchanges/Trading Systems
Are you representing an association?	☐
Country/Region	Germany

Introduction

Please make your introductory comments below, if any

<ESMA_COMMENT_COGL_1>

Deutsche Börse Group (DBG) appreciates the opportunity to respond to ESMA´s consultation paper on „Draft Guidelines on Outsourcing to Cloud Service Providers".

DBG in its capacity as a financial market infrastructure (FMI) provider uses modern IT and technological solutions to operate, and service the financial sector worldwide.

DBG's technologies are at the core of its operations, where they are used to organize the regulated markets, are an integral part of the regulated services we operate. We ensure trust in markets and the efficient functioning of these markets; including but not limited to market data, stock exchange indices, clearing, securities custody, etc.

Regarding new technologies, we are currently working with AI, distributed ledger technology (DLT)/blockchain as well as automation of processes and cloud technology.

We use these technologies in a rather gradual, granular and tested manner, hence continuing to guarantee transparency, stability and investor protection at all times.

We welcome ESMA´s efforts to provide guidance on the outsourcing requirements and the proposed draft guidelines on outsourcing to cloud service providers (CSPs).

In this regard, we want to highlight the following general remarks:

- **Need for a harmonized set of rules for cloud outsourcing**: Different sets of national measures on outsourcing hinder the usage of this technology and the respective services. Developing one EU-wide harmonized set of rules would therefore be relevant not only for the financial sector, but also for the economy as a whole.

- **Use and refer to existing legislation where possible**: As some firms in the financial sector are already following EBA guidelines on outsourcing, ESMA guidelines shall refer to those existing rules where possible and clearly distinct the scope and align to avoid overlaps and incongruencies.
- **Despite market concentration, cloud use must continue to be possible:** The dangers of a strong market concentration with a few non-EU cloud providers. ("lock-in", "data sovereignty" ...), must be actively countered not only on the company side, but primarily on the regulatory one. Risks arising from concentration within the sector need to be evaluated by competent authorities as - due to lacking transparency of such concentration - this is not possible for individual firms. Also, firms do not know and cannot influence the behaviour of other firms to choose a specific CSP in the sector or in other industries.
- **Rethink the risk assessment for outsourcing firms:** Some firms might not be able to fulfil all the requested requirements (e.g. assessment of the political stability the security situation and the legal system, insolvency law analysis), as this would place a burden on outsourcing institutions that is entirely disproportionate to most outsourcing cases.
- **Firms should have the rights to audit a CSP and to ask for expansion of the scope of certifications and audit reports:** in order to fulfil their own requirements with regard to compliance. The use of CSP´s reports should be fully in the firms´ own discretion, but it should not replace current audit rights. Users of CSPs should not be only reliant on the quality of the reports by CSPs. Further, today, some CSPs grant the right to give an expansion of the scope of the certifications or audit reports to other relevant systems and controls of the CSP. However, as of now, contractual arrangements are varying. From a customer perspective, it would be helpful if this would be a legal requirement to grant these requests.
- **Exit plans should be appropriate:** As exit plans do often mean significant efforts (i.e. for migrating application and data), testing may not be possible in many cases. This could be a burden for firms to pick-up the new technology, as e.g. code would need to be rewritten and retested during operations, which would result in very high efforts.
- **Proposal for a sub-outsourcing notification process:** there should be a notification about the CPS´s using sub-outsourcing to allow the customer for an internal risk assessment, including the right to object to the sub-outsourcing and the right to terminate if a CSP would ignore the objection.

Additionally, please find hereunder our detailed DBG comments with regard to the draft guidelines.

In case you have any questions, do not hesitate to reach out to us.

<ESMA_COMMENT_COGL_1>

Questions

Q1 : 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>

As a general remark, in our group, we have several entities, which are following EBA guidelines on outsourcing (e.g. Eurex Clearing AG). Would the ESMA guidelines complement or replace those? Ideally it should be ensured that inconsistencies and duplication of work/reporting is avoided. Therefore, ESMA guidelines should refer to those existing rules where possible and clearly distinct the scope and align to avoid overlaps.

In general, we would agree with ESMA´s proposal for guideline 1, however we have some comments:

- **26 c)** The establishment of an additional outsourcing oversight function needs to be clarified in the context of group structures.
- From our point of view, the description of operational and management functions seems not clearly defined enough.
- **29 l)** We think that the responsibility to identify those sub-outsourcers cannot be in the hands of the firm, as the CSPs would need to inform every single firm which part of their services is sub-outsourced to whom, which might not be possible for CSPs in general with regard to every service. This holds especially true, if the sub-outsourcer is using other providers.
- Further, CSPs are providing only a basic set of information, but not necessarily all of those, which are required for company-internal compliance assessments.
- Risks arising from concentration within the sector need to be evaluated by competent authorities as this is not possible for individual firms. Also, firms do not know and cannot influence the behaviour of other firms to choose a specific CSP in the sector or in other industries.

Further, it seems unclear, what the consequence would be, if an authority would assess a concentration to exceed a certain threshold. Would a company be prohibited to outsource services at some point, while others would be allowed ("first come first serve")? This might contradict competition laws and could harm innovation and damage the level playing field within the EU.

<ESMA_QUESTION_COGL_1>

Q2 : Do you agree with the suggested documentation requirements? Please explain.

<ESMA_QUESTION_COGL_2>
TYPE YOUR TEXT HERE
<ESMA_QUESTION_COGL_2>

Q3 : 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>

Regarding the assessment of relevant risks that may arise as a result of the cloud outsourcing arrangement, we do have the following questions/observations:

- **33 a) vi**: First, why does the analysis also need to include countries within the EU? This may not be in line with the idea of an EU Single Market.
- Second, the requirement to assess the "(…) political stability, the security situation and the legal system, in particular the law, including insolvency law and enforcement as well as the requirements concerning the confidentiality of the firm's business related and/or personal data) (…)" is not adequately defined as regards its scope and the means to achieve it. If the requirement is to be upheld on those broad terms, it will place a burden on outsourcing institutions that is entirely disproportionate to most outsourcing cases.
- This might be an issue for smaller companies to do. Further, if every company interested in outsourcing would assess the political stability, security situation (etc.) of a CSPs origin country on an individual basis with differing criteria this would not only be unproportionate, but would lead to varying outcomes, which complicates the situation for every party involved.
- We would suggest narrowing down the requirement to address the validity and enforceability of the outsourcing contract per se.
- Furthermore, it needs to be taken into account that an insolvency / enforcement analysis will be of theoretical value only given that the insourcing CSP will simply no longer be in a position to provide the contractually agreed services in the case of its own insolvency; data ownership typically is appropriately addressed in CSP agreements.
- **33 a) vii)** Risks arising from concentration within the sector need to be evaluated by competent authorities as this is not possible for individual firms. Also, firms do not know and cannot influence the behaviour of other firms to choose a specific CSP in the sector or in other industries. Further, what would be the consequence, if an authority would assess a concentration above a certain threshold. Would a company be prohibited to outsource services at some point, while others would be allowed ("first come first serve")? This might contradict competition laws and could harm innovation and damage the level playing field within the EU.

GDPR provides already guidance related to that issue in Art. 28 GDPR. The European Data Protection Board and national data protection authorities have already provided guidelines and model contracts in this regard. We see no need for ESMA to further guidance and risk of conflict with future changes in data protection law and jurisdiction. In general, we would recommend referring always to existing regulation.
<ESMA_QUESTION_COGL_3>

Q4 : Do you agree with the proposed contractual requirements? Please explain.

<ESMA_QUESTION_COGL_4>
Referring to the contractual requirements, we have comments to the following issues:

- **41 g)** GDPR provides already guidance related to that issue in Art. 28 GDPR. The European Data Protection Board and national data protection authorities have already provided guidelines and model contracts in this regard. We see no need for ESMA to further guidance and risk of conflict with future changes in data protection law and jurisdiction. In general, we would recommend referring always to existing regulation. Further, in our view there is further clarification needed in terms of data protection, as the text is not precise enough whether referring to personal or general data protection
- **41 h)** We would see the need for further clarification, as we do not understand what exactly has to be monitored. As of now there are several performance monitoring already ongoing.

41 j) In order to fulfil our requirements with regard to compliance, we need to secure the right to audit CSPs. The use of the mentioned reports should be fully in our own discretion, but it should not replace current audit rights. Users of CSPs should not be dependent only on the quality of the reports by CSPs.
<ESMA_QUESTION_COGL_4>

Q5 : Do you agree with the suggested approach regarding information security? Please explain.

<ESMA_QUESTION_COGL_5>

- **44 a) and 45 e)** As exit plans do often mean significant efforts (i.e. for migrating application and data), testing may not be possible in many cases. This could be a burden for firms to pick-up the new technology, as e.g. code would need to be rewritten and retested during operations, which would result in very high efforts.
- **44 c)** might not be feasible in practice since the requirement is quite broad and burdensome for the CSPs in our opinion. CSPs might be expected and willing to offer a kind of "transfer assistance".
- **44 d)** we would like to question how a firm could guarantee that its data is removed/deleted by the CSP. We would only see the solution that the CSP and the outsourcing company would have a contractual agreement to delete the data. Similar provisions are already used in the Art 28 (3) g) of GDPR.

<ESMA_QUESTION_COGL_5>

Q6 : Do you agree with the suggested approach regarding exit strategies? Please explain.

<ESMA_QUESTION_COGL_6>
TYPE YOUR TEXT HERE
<ESMA_QUESTION_COGL_6>

Q7 : Do you agree with the suggested approach regarding access and audit rights? Please explain.

<ESMA_QUESTION_COGL_7>

From our point of view and as a general comment, the approach misses a clear statement that audit rights shall not be limited by contractual obligations, especially not by granting these rights only under certain conditions like in a staggered approach for audits with preconditions to use other information before doing own audits.

Such limiting conditions might be:

- limitation to get audit reports, certificates about compliance to standards;
- requirement to do trainings before getting access rights;
- audits depending of commercial reasonability;
- time and personal constraints;
- limitation to use management consoles; - pre-setting audit procedures.

Towards the details of the approach regarding the access and audit rights, we have comments to the following issues:

- **51 f)** Today, some CSPs grant the right to propose an expansion. However, as of now, contractual arrangements are varying. From a customer perspective, it would be helpful if this would be a legal requirement on the CSP to grant these requests.

<ESMA_QUESTION_COGL_7>

Q8 : Do you agree with the suggested approach regarding sub-outsourcing? Please explain.

<ESMA_QUESTION_COGL_8>

With regard to sub-outsourcing, we have comments to the following issues:

- **55 d)** We agree with this point and would propose the following process: there should be a notification about the CPS´s using sub-outsourcing to allow the customer for an internal risk assessment, including the right to object to the sub-outsourcing and the right to terminate if a CSP would ignore the objection.

<ESMA_QUESTION_COGL_8>

Q9 : Do you agree with the suggested notification requirements to competent authorities? Please explain.

<ESMA_QUESTION_COGL_9>

- In general, ESMA should define critical and important functions in more detail, as NCA´s might interpret these terms differently.
- **58 f)** Please see our comment to point **33 a)** above.

<ESMA_QUESTION_COGL_9>

Q10 : 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>

Q11 : Do you have any further comment or suggestion on the draft guidelines? Please explain.

<ESMA_QUESTION_COGL_11>
TYPE YOUR TEXT HERE
<ESMA_QUESTION_COGL_11>

Q12 : 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>