|  |
| --- |
| 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 | European Association of Co-operative Banks(EACB) |
| Activity | Banking sector |
| Are you representing an association? |[x]
| Country/Region | Europe |

**Introduction**

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

<ESMA\_COMMENT\_COGL\_1>

In general, the guidelines are acceptable, but some issues should be aligned to the reality of CSP. A general requirement on “access-to-premises” is outdated regarding cloud outsourcing. We support the idea that it should be re-defined e.g. as access to the systems, but not physical access to the infrastructure. Also, CSP is a highly standardized approach - technically, commercial and concerning contractual clauses. Individual negotiations and changes to standard agreements are state-of-the-art.

Additionally a general comment on the decision 2016/1250 of the European Court of Justice of 16.7.2020 should be made, as the decision invalidates the EU-US Data Protection Shield agreement and raises a number of question marks concerning "cloud" depending where a cloud services provider (CSP) processes the "outsourced" data (see also Q6.54). However, the ECJ decision is quite new and possible consequences are unclear.

For co-operative banks in Europe, Guideline 6.50 is important, as it mentions (i) usage of third-party certifications and (ii) pooled audits performed jointly with other clients of the same CSP, which helps the model of co-operative banks using "cloud" services of centralized datacenters owned by the co-operative banks together. EACB wants to emphasise this issue, as our “internal” clouds within the co-operative sector are an essential element of the co-operative operating model.

<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>

Yes. However, in 27) a risk-based approach for monitoring is mentioned, but not further specified. If the primary focus should be on the outsourcing of critical and important functions, which risk-based approach would be expected for the rest?

<ESMA\_QUESTION\_COGL\_1>

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

<ESMA\_QUESTION\_COGL\_2>

Ad 28 & 29) the register should contain the same information as for Outsourcing for banking institutions as per the EBA Outsourcing Guidelines. Banks / banking groups have invested and migrated heavily in the past months and, respectively, re-using these developments for the sector of securities operations would be beneficial. A simple reference to the EBA Outsourcing Guidelines for banking institutions would suffice.

<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>

Yes. However, 35) needs to be specified in terms of which certifications would be deemed appropriate.

<ESMA\_QUESTION\_COGL\_3>

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

<ESMA\_QUESTION\_COGL\_4>

Generally, we believe that instead of providing a prescriptive set of what needs to be included in a contract, SCCs would have been a better approach for CSPs and firms.

Concerning point 41.f) we would like to point out that listing the countries where the CPSs’ data centres reside will not be sufficient to cover the complete process of ‘storing and processing’ of data.

On a more general note, the requirements of Guideline 3 might be quite hard to implement for certain outsourcing activities. Especially large CSP like AWS, Microsoft Azure, or Google Cloud offer standard services and might not always enter into details and negotiate every aspect of the service. Even though the standard service covers most of the aspects expected by the Guideline 3, they are not tailored to the needs of the firm outsourcing the service.

<ESMA\_QUESTION\_COGL\_4>

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

<ESMA\_QUESTION\_COGL\_5>

Ad 43.c) Please provide more examples for appropriate key management solutions. Preventing the CSP from storing and managing encryption keys is not covering all types of cloud solutions nor is it probable that large CSPs would accept additional contractual conditions for separation of duties between key management and operations, if these aren’t already covered by their standard contractual templates for standardized cloud solutions (e.g. within public clouds).

<ESMA\_QUESTION\_COGL\_5>

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

<ESMA\_QUESTION\_COGL\_6>

Generally, yes.

Ad 44.a) “Testing” an Exit Plan will not work in many cases. Such a “testing” is also not required in other outsourcing guidelines or supervisory requirements.

Ad 44.c) This is generally not part of the standard service of e.g. AWS, Microsoft Azure, or Google Cloud and might be hard to impose. Operators like AWS, MS Azure and Google Cloud Platform cannot perform the exit on behalf of the customer, because they have no contractual arrangement with any other CSP. Realistically, any obligations can only concern a transfer of the data back to the customer (and to proceed with 44 b).

<ESMA\_QUESTION\_COGL\_6>

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

<ESMA\_QUESTION\_COGL\_7>

The differentiation between “access” and “audit” is unclear. Access without audit right makes no sense and vice versa. Instead state that any “audit right” includes “access right”. A general requirement on “access-to-premises” is outdated regarding CSP. We support the idea that “access” should be defined e.g. as access to the systems or services, but not physical access to the infrastructure.

Points 50) ff in principle put the whole responsibility to every company individually to assess, if provided certifications, etc. are appropriate to ensure proper auditing. As outlined above and regarding point 35), the Guidelines should provide a list of international certificates that are deemed proper to cover processes, applications, infrastructure, data centers.

In point 50a) the wording “may use” (certifications etc) for non-critical outsourcings: does that mean certifications etc will *replace* further audit activities?

51f) seems not feasible to be handled with on the individual company level.

<ESMA\_QUESTION\_COGL\_7>

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

<ESMA\_QUESTION\_COGL\_8>

As regards point 55.3, having the right to object a material subcontractor does not reflect “real life” commercial agreements. None of the CSPs could grant this right without jeopardizing their business. Instead of objecting, the cloud service user should be informed in time and have the right to terminate the contract.

<ESMA\_QUESTION\_COGL\_8>

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

<ESMA\_QUESTION\_COGL\_9>

Generally, yes. However, we believe that Guideline 8 should also be addressed to competent authorities as the CA should set the provisions for notifications, provide the templates etc.

<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>

Yes, we do have general concerns about the approach.

First, it is unclear why the guidelines are narrowed down to *Cloud* Outsourcing and not Outsourcing (incl. Cloud) in general. For banking institutions, Outsourcing and Cloud was combined already (since the EBA Outsourcing Guidelines explicitly include cloud outsourcing activities).

Second, it seems that Outsourcing raises the same risks for credit institutions as for investment firms or any other financial institutions. If so, there should be the same rules for all of them (e.g. by a Joint Guideline on Outsourcing from ESMA & EBA). The current approach (Outsourcing Guidelines incl Cloud for banking institutions, slightly different Cloud Outsourcing Guidelines for securities firms) will lead to complexity and additional bureaucracy.

Additionally, we observed that even the definitions used in the ESMA draft Guidelines seem to deviate (slightly) compared to the recent EBA Guidelines (critical / important function; cloud), which does not provide for a consistent approach.

<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>

The answer depends on the specification of above outlined unclear topics (e.g. risk-based approach, contractual requirements, audit, etc.). Depending on specification, additional resources in overall governance as well as in the specific functions (IT, Security, Procurement / Outsourcing, Legal, etc.) may be needed to comply with the Guidelines.

<ESMA\_QUESTION\_COGL\_12>