31 August 2020

**EACB response to the**

**ESMA Consultation Paper on**

**Draft Guidelines on Outsourcing to Cloud Service Providers**

The **European Association of Co-operative Banks** ([EACB](http://www.eacb.coop/en/home.html)) represents, promotes and defends the common interests of its 27 member institutions and of cooperative banks, with regard to banking as well as to co-operative legislation. Founded in 1970, today the EACB is a leading professional lobbying association in the European banking industry. Co-operative banks play a major role in the financial and economic system. They contribute widely to stability thanks to their anti-cyclical behaviour, they are driver of local and social growth with 2.800 locally operating banks and 51,500 outlets, they serve 209 million customers, mainly consumers, SMEs and communities. Europe’s co-operative banks represent 84 million members and 713,000 employees and have an average market share in Europe of about 20%.

For further details, please visit[www.eacb.coop](http://www.eacb.coop)

**General Comments**

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 A general requirement on “access-to-premises” is outdated regarding cloud outsourcing.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

**Answers to the different 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.*

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?

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

Ad 28 & 29) the register should contain the same information as for Outsourcing for credit institutions as per the EBA Outsourcing Guidelines. Firms / banking groups have invested and migrated heavily in the past months and re-using it for security subsidiaries / customers would be beneficial. A simple reference to the EBA Outsourcing Guidelines for credit institutions would suffice.

*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.*

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

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

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 ‘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 when engaging with large CSP like AWS and Azure, they 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.

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

Generally, yes.

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 big 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).

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

Generally, yes.

Ad 44.a) “Testing” the Exit Plan will not work in many cases. This would be too expensive, risky and time-consuming.

Ad 44.c) This is generally not part of the standard service of AWS and Azure 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).

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

No.

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”.

Points 50) ff are in principle imposing the whole responsibility to each and every company 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.

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

As regards point 55.3, having the right to object a material subcontractor does not reflect ‘real life’ (although it is a long-term supervisory requirement). None of the CSPs could grant this right without jeopardizing their business. Instead of objecting, the firm should be informed in time and have the right to terminate the contract.

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

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.

*Q10: Do you agree with the suggested approach regarding the supervision of cloud outsourcing* *arrangements by competent authorities? Please explain.*

Yes.

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

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 as such. For credit 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 credit 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.

*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 organisation, where relevant.*

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.