Reply form for the EBA Consultation Paper on Draft Recommendations on Cloud Outsourcing

Confidential

Date: 18 August 2017

Responding to this paper

The EBA invites comments on all proposals put forward in this paper and in particular on the specific questions summarised in 5.2.

Comments are most helpful if they:

- respond to the question stated;
- indicate the specific point to which a comment relates;
- contain a clear rationale;
- provide evidence to support the views expressed/ rationale proposed; and
- describe any alternative regulatory choices the EBA should consider.

Submission of responses

To submit your comments, click on the 'send your comments' button on the consultation page by 18.08.2017. Please note that comments submitted after this deadline, or submitted via other means may not be processed.

Publication of responses

Please clearly indicate in the consultation form if you wish your comments to be disclosed or to be treated as confidential. A confidential response may be requested from us in accordance with the EBA rules on public 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 the EBA Board of Appeal and the European Ombudsman.

Data protection

The protection of individuals with regard to the processing of personal data by the EBA is based on Regulation (EC) N° 45/2001 of the European Parliament and of the Council of 18 December 2000 as implemented by the EBA in its implementing rules adopted by its Management Board. Further information on data protection can be found under the Legal notice section of the EBA website.

Association of Financial Markets in Europe (AFME)

The Association for Financial Markets in Europe (AFME) welcomes the opportunity to share our views on the Consultation Paper issued by the European Banking Authority (EBA) published on 18 May 2017, with a deadline for a response by 18 August 2017.

AFME represents a broad array of European and global participants in the wholesale financial markets. Its members comprise pan-EU and global banks as well as key regional banks, brokers, law firms, investors and other financial market participants. We advocate stable, competitive, sustainable European financial markets that support economic growth and benefit society.

AFME is the European member of the Global Financial Markets Association (GFMA) a global alliance with the Securities Industry and Financial Markets Association (SIFMA) in the US, and the Asia Securities Industry and Financial Markets Association (ASIFMA) in Asia. AFME is listed on the EU Register of Interest Representatives, registration number 65110063986-76.

Please do not hesitate to contact Emmanuel Le Marois on 44 203 828 2674, email Emmanuel.LeMarois@afme.eu, or David Ostojitsch on 44 203 828 2761, email David.Ostojitsch@afme.eu, should you wish to discuss any of the points.

Executive Summary

AFME welcomes the opportunity to support the EBA on the draft recommendations on cloud outsourcing, as part of a broader effort being undertaken by European Institutions to update these practices across the EU.

The transition to cloud is increasingly important for developing robust and efficient wholesale financial markets, and requires all industry participants to address the risk of potential regulatory fragmentation across jurisdictions that may increase in the industry, as cloud service uptake increases and associated policy is developed.

Overall AFME is in broad agreement on the intent of the proposed EBA cloud outsourcing guidelines as a measured approach to proportionally balance risk and complexity, while promoting flexibility to support increased future cloud adoption.

In summary of our response to this proposal:

- The EBA should not look to introduce new requirements or restrictions beyond existing outsourcing regulations;
- The provided guidance should remain technology and entity neutral, i.e. should be applied equally across Financial Institutions (FIs), FinTech companies, and Financial Market Infrastructure (FMI) and other related participants using such technology;
- The guidelines highlight the increasing need for the education of, and collaboration between, FIs, Cloud Service Providers (CSPs) and policymakers;
- Global harmonisation is key to the adoption of cloud technology, particularly for firms operating in multiple jurisdictions;
- AFME proposes an alternate recommendation for supporting the EBA guidelines for access and audit rights, which leverages existing industry standards and certifications for supervisory requests (e.g. ISO 27001, 27002 and 27018);
- Regarding scope, we urge the EBA to recognise that certain types of cloud service engagements should not be considered outsourcing in the traditional sense and recommend that the EBA take account of this in its forthcoming revision of CEBS 2006 outsourcing guidelines.

AFME looks forward to the opportunity to continue supporting the EBA towards the publication of the guidelines in Q4 2017.

Question 1: Are the provisions from these recommendations clear and sufficiently detailed to be used in the context of cloud outsourcing?

1. Compliance and reporting obligations:

   1.1. Confirming that no response is requested for section 1.

2. Subject matter, scope and definitions:

   2.1. AFME is supportive of the EBA risk based approach to cloud, allowing for a technology neutral approach to its guidance and future proofing recommendations. However, AFME's view is that the EBA guidance should focus on the nature of engagements between Cloud Service Providers (CSPs) and Financial Institutions (FIs). In doing so, it may recognise that certain types of cloud engagement are not outsourcing in the traditional sense.

   2.2. Outsourcing requirements are tailored to the context of a third party performing a business activity or process on behalf of an FI. However, in an IaaS context for example, the FI is only "outsourcing" the underlying infrastructure, while retaining control of the relevant business activity or process for which that underlying infrastructure is required. In this way, IaaS is more aligned to "buying-in" the supply of a commodity or tool, rather than the outsourcing of an activity or process. Revising outsourcing guidance based on these reasons, i.e. the different types of engagements and services exchanged between FIs and CSPs, would not violate the EBA technology neutral approach.

   2.3. AFME believes that to fully realise the benefits and appropriately mitigate the risks of cloud outsourcing, further education and collaboration on cloud requirements with the broader financial services eco-system, such as CSPs, is required. Although CSPs are not subject to direct oversight by National Competent Authorities (NCAs), FIs are contractually required to ensure access to authorities for supervisory and auditing purposes. Further education with CSPs would help ensure support and compliance in this process.

   2.4. AFME believes that further clarification on how systemic risks should be managed (e.g. domestic and international), and how to achieve third-party certification (e.g. paragraph 8(b)), would support harmonisation of practices across Europe and promote financial stability.

3. Implementation

   3.1. Confirming that no response is requested for section 3.

4. Recommendations on outsourcing to cloud service providers

4.1. Materiality assessment

4.1.1. AFME is supportive of a risk based approach for materiality assessment in the proposed guidelines. Cloud outsourcing risks may depend on a variety of factors such as the type of cloud solution adopted, the type of activity outsourced, a firm's size or

structure; therefore, a risk based approach seems appropriate to define risk assessments and associated controls required.

4.1.2. AFME is supportive of a technology-neutral approach to cloud outsourcing and would like to stress that more restrictive interpretations of "materiality" should not be introduced beyond the current CEBS guidelines. AFME supports continuation of the flexibility required for a risk based approach that can adequately address the continuously evolving landscape of cloud outsourcing risks.

4.2. Duty to adequately inform supervisors

4.2.1. AFME is supportive of informing on material activities outsourced to CSPs, however this should be at an appropriate level and intent, rather than case-by-case authorization. A requirement for case-by-case authorization may create supervisory bottlenecks and increase time to market without material supervisory benefit. We recommend the EBA avoid duplicative reporting requirements by leveraging existing reporting and notification processes wherever possible, if such reporting already effectively communicates the pertinent outsourcing information to the competent authority.

4.2.2. Furthermore, AFME believes there is a risk of data duplication and fragmentation if individual NCAs can request additional information on CSPs without consulting or aggregating data that FIs have already provided and may be readily available. Similarly, the level of information required at the institution and group level may further emphasize data quality risks.

4.2.3. With regards to specific guidance in the EBA consultation:

4.2.3.1. Location of data: AFME believes that emphasis on data location will remain important and evolve with changing technologies, such as encryption, data partitions or distributed ledgers. FIs will continue to focus on how data locations are managed and the controls required, regarding CSPs and data jurisdictions.

4.2.3.2. Business Continuity Plans: AFME believes that Business Continuity Plans (BCP) should be completed and assessed according to the size, structure and specific activities performed by the outsourcing FIs, which would be in accordance with the principle of proportionality. There may be a risk of diverging contractual requirements and fragmentation if NCA's were to view Business Continuity plans and subsequently develop contractual requirements for cloud outsourcing.

4.2.3.3. Maintenance of an updated register: AFME believes that appropriate mitigation and controls for cloud outsourcing should be dictated by the principle of proportionality. Therefore, it should be the responsibility of FIs to determine appropriate documentation, management and oversight in relation to its organisational structure.

4.2.3.4. Information to be included in the register: AFME views that the guidance in its current form (e.g. "should at least be included") could encourage "gold plating" from Member States, potentially creating divergence from the EBA objective of harmonisation.

4.2.4. Furthermore, AFME views that providing specific category names for the type of cloud outsourcing technology used (e.g. "IaaS, PaaS, SaaS, public/private/hybrid/community") creates an unnecessary burden to continuously monitor and update a restricted list, reducing the guidance's objective of being future proof.

4.2.5. Finally, the use of prescriptive and vague terms (e.g. "easy, difficult or impossible") creates ambiguity which could be subjectively interpreted by NCAs. AFME views that explicit definitions would provide further clarity and recognised methods for quantification, and would support the EBA in the determination of these terms.

4.3. Access and Audit rights

For institutions

4.3.1. AFME views that the requirements for securing rights to access and audit could be an obstacle for financial institutions when outsourcing to Cloud Service Providers (CSPs):

4.3.1.1. Unrestricted right of inspection may potentially create unnecessary operational risks to CSPs and should therefore be timely and relevant to the service provided to the regulated entity;

4.3.1.2. Providing access to business premises may have limited benefits. Currently for security and resiliency purposes data may be held in various locations leveraging encryption and data partitioning techniques. Therefore, physical access should be specific to the sites where the service provided is deemed most relevant to the regulated entity (see point 4.2.2 – location of data);

4.3.1.3. AFME proposes an alternative approach to allow for a more balanced and proportionate solution; to satisfy access and audit rights requirements while addressing risks and concerns regarding outsourced activities:

4.3.1.4. The use of either pooled audits or third-party certifications (as stated in the EBA proposals 4.3.8);

4.3.1.5. Rights to access and audit could be addressed by allowing outsourcing institutions to leverage existing industry standards and certifications of CSPs (e.g. ISO 27001, 27002 and 27018), that broadly cover the EBA requirements;

4.3.1.6. The CSP could provide certification and reports reflecting the scope of services provided (i.e. statement of applicability) providing insurance that the EBA requirements for access and audits are satisfied.

4.3.2. Regarding access and audit rights, AFME views that the EBA guidance should make explicit that:

4.3.2.1. The use of either pooled audits or third-party certifications (para. 8) sufficiently meet the requirement of audit and access rights (para. 6);

4.3.2.2. The term "where an outsourcing institution does not employ its own audit resources" is intended to mean "where an outsourcing institution chooses not to employ its own audit resources". This would help clarify that Financial Institutions (FIs) with audit resources are not prevented from this optionality.

4.3.3. AFME believes that to achieve appropriate controls to mitigate cloud outsourcing risks while minimising operational risks, FIs, CSPs and policy makers should work towards reporting standards and industry best practices. These would allow firms to

take a risk based approach while ensuring certifications and audits meet regulatory requirements.

4.3.4. Regarding certification, the work conducted in 2015 by ENISA together with the Cloud Select Industry Group on Certification Schemes and the European Commission regarding the "Cloud Certification Schemes Metaframework (CCSM)" should be welcomed as well as the standards promoted by the NIS Directive. The CCSM maps out detailed security requirements used in the public sector to describe security objectives in existing cloud certification schemes.

4.3.5. However, a step further should be undertaken to coordinate the development of sets of certifiable controls as part of the STAR certification and the SSAE 16 type II, which is an internationally recognised standard to audit on security and governance as well as the CSA's Guidance and Cloud Controls Matrix which maps CSA recommendations against other control frameworks including ISO 27001/2, BITS v5/6 and ENISA IAF.

For competent authorities

4.3.6. AFME believes the EBA should clarify that "business premises" is not intended to mean "data centres", as indicated in its public hearing of 20th June 2017.

4.4. In particular for the right of access

4.4.1. AFME believes that further clarification is required regarding the terms "business premises", "reasonable time" and "due to an emergency or crisis" as these may introduce subjective interpretation from NCAs, and therefore a risk of fragmentation across Member States. Developing Industry best practices may help support defining these terms. AFME would welcome the opportunity to support the EBA in determining the terms listed above.

4.5. Security of data and systems

4.5.1. AFME recommends that the EBA, as explained in its consultation, clearly positions its recommendations in line with existing regulation on security incident management and reporting, to avoid overlaps with existing regulations or setting new criteria, such as the Directive on Network and Information Systems (NIS)[1], the EU General Data Protection Regulation (GDPR)[2] or EU Payment Services Directive 2015/2366 (PSD2)[3];

4.5.2. AFME views that the EBA contractual requirement should be amended as follows; "the outsourcing contract should oblige the CSP to protect the confidentiality of the information transmitted by the FI *to the degree appropriate to the type of engagement"*. The extent to which a CSP is in control of a FIs data, and therefore the appropriate controls, will vary depending on the type of engagement between the CSP and FI. For example, while the CSP may receive and control a FIs customer data in certain service agreements, there are others where a CSP may receive encrypted FI customer data but no key, meaning the FI retains control of the data.

[1] https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive
[2] http://ec.europa.eu/justice/data-protection/reform/index_en.htm
[3] https://ec.europa.eu/info/law/payment-services-psd-2-directive-eu-2015-2366_en

4.5.3. AFME views an increase in risks to security and data privacy if encryption methods and associated keys are provided to potentially multiple regulators without appropriate controls and protocols. Where it is necessary for a regulator to perform its supervisory duty, AFME believes FIs and CSPs should provide regulators access to underlying data, however access to key and encryption should be restricted if not discouraged.

4.5.4. See AFME's response to section 4.3. "Access and Audit rights - For institutions" regarding requirements for securing right to access and audit. In summary;

4.5.4.1. Unrestricted right of inspection may potentially create unnecessary operational risks to CSPs;

4.5.4.2. Providing access to business premises may have limited benefits;

4.5.4.3. AFME supports the EBA proposal of using either pooled audits or third-party certifications (as stated in the EBA proposals 4.3.8).

4.6. Location of data and data processing

4.6.1. AFME welcomes the EBA view that data processing outside of the EEA should be subject to a risk based approach as equal to data processed inside the EEA;

4.6.2. AFME recommends that the guidance emphasize in this section that CSPs should ensure, without unnecessary extra costs and limitations, the effective migration of data to another CSP upon request. Moreover, CSPs should ensure regulated entities can meet regulatory compliance such as requirements on data subject rights, as set forth in the GDPR (e.g. right to data portability, right to erasure), where data subjects can exercise their right towards data controllers (i.e. the outsourcing institutions).

4.7. Chain sourcing

4.7.1. AFME views a clear distinction between the responsibilities of the outsourcing institution and the CSP in chain sourcing arrangements:

4.7.1.1. The outsourcing institution (e.g. the FI) should be responsible for the review and monitoring of the CSPs performance against its contractual obligations;

4.7.1.2. The CSP should be responsible for the review and monitoring of any subcontractors it has engaged to meet its contractual obligations with the FI;

4.7.2. Regarding chain outsourcing, the EBA should a provide specific clarity that:

4.7.2.1. To ensure comfort with a CSP's subcontractors, of which there are often many, it is sufficient for an FI to review a CSP's third-party oversight processes;

4.7.2.2. The guidance only applies to subcontractors connected to a CSP's provision of services to FIs.

4.7.3. Industry led standards for CSPs and relevant subcontractors aiming to provide services to FIs, and industry led standards on what is required from a financial services perspective, would be helpful. This would reduce the friction between an outsourcing

institution and CSP, while addressing the objectives of this section. An example industry standard for context is ISO37500:2014, which provides guidance on outsourcing process and governance.

4.7.4. See AFME's answer to section 4.5. "Security of data and systems" regarding the proposed guidance notes that "the outsourcing contract should oblige the CSP to protect the confidentiality of the information transmitted by the FI".

4.7.5. See AFME's response to section 4.3. "Access and Audit rights - For institutions" regarding requirements for securing right to access and audit. In summary;

4.7.5.1. Unrestricted right of inspection may potentially create unnecessary operational risks to CSPs;

4.7.5.2. Providing access to business premises may have limited benefits;

4.7.5.3. AFME supports the EBA proposal of using either pooled audits or third-party certifications (as stated in the EBA proposals 4.3.8).

4.8. Contingency plans and exit strategies

4.8.1. AFME believes setting up robust contingency plans and exit strategies are key to increase trust, resilience and therefore adoption of cloud outsourcing. AFME believes FIs should work more closely to define an approach which would take into consideration the size, type and activity outsourced with a view of defining industry best practices based on proportionality and risk mitigation. For context, the approach could determine the appropriate plans required for production and test activities in the cloud, which may have differences in both scale, criticality and length of time the environment may be in use.

4.8.2. Currently the proposed guidance requires that FIs exits plans are sufficiently tested where appropriate. AFME believes that testing exit plans in practical sense may be an overly burdensome exercise, hindering the adoption of cloud across the region. EBA should clarify that non-practical testing of exit strategies is "sufficient" as required by the proposed guidance.

Question 2: Are there any additional areas which should be covered by these recommendations in order to achieve convergence of practices in the context of cloud outsourcing?

a. AFME sees potential in further collaboration between FIs, CSPs, the EBA and policy makers to combine efforts on standards for:
   i) Reporting;
   ii) Audit and access rights;
   iii) Exit plans.

b. As a key issue which requires resolution for firms operating in the EU and across other jurisdictions, AFME would welcome more reference to global harmonisation efforts in the EBA guidelines.

c. Example challenges identified by AFME with regards to global harmonisation of cloud outsourcing include:
   i) Which regulation(s) would take precedence with respect to data access, audit, monitoring, data lineage and any cross-border data migration?
   ii) As CSPs are emerging across financial markets how do they on-board across the various regulatory stipulations and guidelines?

d. AFME would welcome in the EBA guidelines more reference to key EU regulatory requirements which could potentially have a significant impact on cloud computing, such as the Directive on Network and Information Systems (NIS)[4], the EU General Data Protection Regulation (GDPR)[5] or EU Payment services Directive 2015/2366 (PSD2)[6]; ensuring that further granularity on these guidelines are supportive and harmonised within this broader regulatory context.

e. AFME welcomes the opportunity to comment and would appreciate the opportunity to discuss this important consultation. Please do not hesitate to contact Emmanuel LeMarois (Emmanuel.LeMarois@afme.eu), or David Ostojitsch (David.Ostojitsch@afme.eu), should you wish to discuss any of the above.

[4] https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive
[5] http://ec.europa.eu/justice/data-protection/reform/index_en.htm
[6] https://ec.europa.eu/info/law/payment-services-psd-2-directive-eu-2015-2366_en