European Association of CCP Clearing Houses

EACH response to the ESMA Consultation Paper 'Draft Guidelines on Outsourcing to Cloud Service Providers'

September 2020

European Association of CCP Clearing Houses AISBL (EACH), Avenue des Arts 6, 1210 Brussels

Introduction

The European Association of CCP Clearing Houses (EACH) represents the interests of Central Counterparties (CCPs) in Europe since 1992. CCPs are financial market infrastructures that significantly contribute to safer, more efficient and transparent global financial markets. EACH currently has 19 Members from 15 different European countries. EACH is registered in the European Union Transparency Register with number 36897011311-96.

EACH appreciates the opportunity to provide feedback to the ESMA consultation paper "Draft Guidelines on Outsourcing to Cloud Service Providers" (hereinafter called "The consultation").

Some **general remarks** that EACH would like to express regarding the outsourcing to Cloud Service Providers (CSPs) are the following:

- **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 an EU-wide harmonized set of rules would therefore be relevant not for the financial sector, but also for the economy as a whole. We would, in addition, recommend ESMA to refer to the already existing legislation where possible.
- **Clear guidance based on existing rules** – For companies, a clear guidance based on existing rules would be beneficial. Further, there is a clear need for EU rules covering cloud outsourcing, which on the one hand promote the uptake of the technology to make the financial industry more competitive and on the other hand incorporate existing standards (e.g. the German BSI C5 standard), which are already used by the industry.
- **Integration of ESMA guidelines in existing Technology Strategy, Vendor Management, Procurement and Information Security processes** – Companies often see outsourcing to CSPs as part of their Technology Strategy and is best placed within this strategy to ensure a holistic approach towards the use and oversight of technology. A standalone cloud strategy or policy will not be necessarily beneficial towards the better governance and oversight of the use of CSPs. Companies currently have an outsourcing policy in place that covers oversight, monitoring, pre-engagement due diligence and risk analysis of any outsourcing; these policies and processes also cover outsourcing to CSPs. The outsourcing policy aligns with existing group processes for Vendor Management, Procurement and Information Security. Therefore, outsourcing to CSPs does not necessarily require its own strategy. Therefore, EACH would recommend that any **final ESMA Guidelines on outsourcing to CSPs should be allowed to be integrated into the firms' existing Technology Strategy, Vendor Management, Procurement and Information Security processes** to avoid the creation of a new and redundant cloud standalone structure.
- Additionally, EACH believes that ESMA should explicitly recognize the qualitative differences between a firm outsourcing tasks to an unaffiliated third party and tasks being performed in connection with shared services among affiliates. When tasks are performed as shared service, there is an alignment of the interest from the firm's side in meeting its responsibilities and those performing tasks because the ultimate

shareholders are the same. By contrast, when a third party performs tasks on behalf of a firm there is no such alignment of interests. Importantly, as ESMA notes, the firm retains full responsibility, legal liability and accountability to the regulator for all tasks. Therefore, EACH would recommend that any **final ESMA Guidelines on CSP should reflect the difference between a firm outsourcing tasks to an unaffiliated third party and tasks being performed in connection with shared services among affiliates.**

- **Problems/risks of the current cloud market** – Asymmetry of power of negotiation between customer and CSPs – i.e. high efforts and time are required to agree regulatory compliant contracts with CSPs in the financial sector – are detrimental for the current cloud market. Therefore, EACH actively supports the EU work designing "Voluntary Standard Contract Clauses" to facilitate future negotiations. Also, EACH believes it is very difficult to procure/adopt new and innovative cloud solutions, as it takes a long time to ensure that these new services are compliant with the regulations. Often, new solutions do not meet regulatory expectations right from the start. Therefore, in order to be competitive at global level and attract investments, independent EU cloud structures should be created where possible.
- **Despite market concentration, cloud use must continue to be possible** – The dangers of a strong market concentration with a few non-EU cloud providers ("data sovereignty" ...), must be actively countered not only on the company side, but primarily on the regulatory one. However, mandatory and prescribed measures to reduce the risk of concentration (e.g. cyclical changes of provider) are not appropriate, as they do not address the underlying problem. Instead, Europe-wide standards for cloud technology should be established (e.g. in the areas of outsourcing, data protection or access rights), based on European values and serving as a guideline for third-country providers.
- **Proportionality** – EACH welcomes the intention of ESMA to take into account proportionality when drafting these guidelines by e.g. differentiating between critical or important functions and non-critical or important functions, with the objective of taking into account the risk underlying the outsourcing of those functions.

Guideline 1. Governance, oversight and documentation

Q1. Do you agree with the suggested approach regarding a firm's governance and oversight in relation to its cloud outsourcing arrangements? Please explain.

As a first comment, we would like to stress the necessity to clarify whether the ESMA guidelines on outsourcing to cloud service providers are meant to complement or substitute the EBA guidelines on outsourcing arrangements[1], and whether CCPs with a banking licence should follow either the EBA or the ESMA guidelines. In this regard we believe that, ideally, inconsistencies as well as duplication of work or reporting are to be avoided.

[1] https://eba.europa.eu/sites/default/documents/files/documents/10180/2551996/38c80601-f5d7-4855-8ba3-702423665479/EBA%20revised%20Guidelines%20on%20outsourcing%20arrangements.pdf

In general, we agree with the statement in **paragraph 25** that firms should have a defined and up to date cloud outsourcing strategy, which should be consistent with strategies including information and communication technology strategy, information security strategy, operational risk management strategy, and internal policies and processes. We further support that, in **paragraph 26**, the proposed guidelines establish that firms should:

a) clearly assign the responsibilities for the documentation, management and control of cloud outsourcing arrangements within its organisation;
b) allocate sufficient resources to ensure compliance with these guidelines and all of the legal requirements applicable to its cloud outsourcing arrangements;
c) establish an outsourcing oversight function or designate a senior staff member who is directly accountable to the management body and responsible for managing and overseeing the risks of cloud outsourcing arrangements. However, it is our opinion that the establishment of an additional outsourcing oversight function needs to be clarified in the context of group structures.

Regarding **paragraph 29**, we would like to point out that CSPs provide only a basic set of information, but not necessarily all of those listed in the paragraph, which are required for company-internal compliance assessments. In particular, referring to point 29(l) we believe it is not possible for the outsourcing firm to provide a full list of all sub-outsourcer, as hyperscale CSPs use a long list of sub-contractors that may be used e.g. in specific support cases.

Furthermore, regarding **point 29(a)**, we argue that the use of a reference number is limiting, and an alphanumeric code or another reference might be more appropriate. Therefore, in the case of reference number we suggest that **the final Guideline 1 should only require the use of a reference.**

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

We would like to get further clarity on the length of time that a firm would be required to maintain a record of terminated cloud outsourcing arrangements. Additionally, EACH has reservations to create a standalone single register for outsourcing to CSPs. Companies' Vendor Management assess the vendor's criticality and risk against companies' common enterprise risk policy. Companies normally maintain a common enterprise risk register and outsourcing agreements to CSPs constitute part of this register. We would argue that cloud is just another technology and the creation of a separate register would not improve the governance or oversight of this technology within firms.

Therefore, EACH suggests that the **final Guideline 1 should require firms to maintain the relevant information on outsourcing agreement of CSP in registers**, **however the final Guideline 1 should not require to create a new and separate, standalone register just for outsourcing to CSPs.**

EACH would like to also propose the following amendments:

- As regards the criticality test that shall be conducted in relation to the function that will be subject to outsourcing, we suggest that ESMA clarifies in paragraph 28 that such **assessment should be based on and limited to the criteria set out in the definition**

of "critical functions" included in the Guidelines. This would help ensure standardised evaluation across different entities and supervisory practices.

- Concerning the relevant information that should be included in the register – referred to in paragraph 29 - we suggest that ESMA clarifies whether the **CSP is subject to any law or regulations which would allow third parties, including agencies or supervisory authorities, request access to the firm's data.** This would help to preserve confidentiality of firm's data.

Guideline 2. Pre-outsourcing analysis and due diligence

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.

We agree with ESMA's guidelines on pre-outsourcing analysis and due diligence to be conducted on a prospective CSP, and that this should be proportionate to the nature, scale and complexity of the function that is being outsourced. However, when it comes to the assessment of relevant risks that may arise as a result of the cloud outsourcing arrangement (paragraph 33, point a), we would like to put forward the following observations:

- **Paragraph 33(a)(vi)**
  - 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.
  - Performing such analysis on the political stability, the security situation, and the legal system of the country in which the outsourced functions would be provided might represent an issue for smaller companies. Further, if every company interested in outsourcing had to assess the above-mentioned aspects of a CSPs' country of origin on an individual basis, it is highly likely that differing criteria would be used. This would not only be disproportionate, but would lead to varying outcomes, complicating the situation for every party involved. We would therefore 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 the position to provide the contractually agreed services in the case of its own insolvency.
- **Paragraph 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

consequences of an authority possibly assessing concentration above a certain threshold? Would a company be prevented from outsourcing services, while others would be allowed to outsource ("first come, first served")? This might contradict competition laws and could harm innovation, as well as damage the level playing field within the EU.

Guideline 3. Contractual requirements

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

EACH agrees that the rights and obligations of a firm and of its CSP should be set out clearly in a written agreement, especially for what concerns the outsourcing of critical and important functions. Nevertheless, we would like to put forward the following comments with regard to paragraph 41:

- **Paragraph 41(f)**
  - We recommend adding back-up data as the relevant data. In addition, along with the notification to the firm in case the CSP proposes to change the location(s), an obligation to notify any request for access to data by the Authorities should be added.
- **Paragraph 41(g)**
  - Article 28 of the GDPR[2] already provides guidance on provisions concerning information security and personal data protection, and the European Data Protection Board as well as national data protection authorities have already provided guidelines and model contracts in this regard. We therefore do not see the need to put forward further guidance and incur in potential risk of conflict with future changes in data protection law and jurisdiction.
  - In addition, in our view there is further clarification needed in terms of data protection, as the text is not precise enough on whether referring to personal or general data protection. Both topics are indeed distinct from each other, as personal data protection is covered in GDPR and general data protection is covered in other rules and regulation (e.g. the NIS-Directive[3]).
- **Paragraph 41(h)**
  - EACH believes that clarifications are needed as regards how a firm could monitor the CSP's performance on a regular basis. Currently, several performance monitoring exercises are already in place.
- **Paragraph 41(j)**
  - To fulfil the requirement under paragraph 41(j), we would need to secure the right to audit CSPs. The use of the mentioned reports should be fully at the firm's own discretion but should not replace current audit rights. In addition, the users of CSPs should not be dependent only on the quality of the reports by CSPs.

[2] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN
[3] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN

- **Paragraph 41(k)**
  - We suggest specifying that the CSP must report incidents including cyber incidents in case where the supervised entity is subject to the regulatory obligation of reporting of incidents (e.g. in compliance with the NIS Directive).

Guideline 4. Information security

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

EACH generally agrees with ESMA's approach regarding information security and considers the list of requirements suggested in Guideline 4 as a solid basis of a good security implementation for cloud projects. However, we would caution against prescriptive language, as that could be perceived as being contrary to the stated risk-based approach. Therefore, EACH suggests that **the final Guideline 4 be adjusted by using "evaluate, assess, or consider" (suggesting best practice) instead of the current "ensure" (suggesting a prescriptive requirement)**, as it would help clarify that the actual intent is to provide a roadmap of topics to consider following a risk-based approach.

Additionally, EACH suggests that IT security should be clearly distinguished from data protection, as the two concepts have different implications, and would encourage ESMA to use the already existing terminology.

Regarding paragraph 43 (f), on business continuity and disaster recovery – we note that this is also relevant for operational resiliency in general and not only information security.

Guideline 5. Exit Strategies

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

As a first comment, we would suggest that harmonisation is maintained on guidance and rules from different authorities on exit strategies relating to cloud outsourcing.

In general, EACH agrees with the proposed guidance that a firm's exit plans should be comprehensive, documented and sufficiently tested, but EACH Members believe that the following points in paragraphs 44 and 45 need some further consideration:

- **Paragraphs 44(a) 44 (b) and 45(e)**
  - As exit plans often imply significant work (i.e. for migrating application and data), in many cases testing may not be possible. This could be a burden for firms to pick-up the new technology, as e.g. codes would need to be rewritten and retested during operations, which would result in very high efforts. We therefore believe that a risk-based and proportionate approach is required when testing exit strategy. Exit strategies can be reliably estimated based on

foundational capabilities such as landing zones in the alternative CSP. Hence, we would suggest that these foundational capabilities be required to be tested for compatibility and the gaps documented.

- **Paragraph 44 (c)**
  - This requirement might not be feasible in practice. CSPs might be willing to offer a sort of "transfer system".
- **Paragraph 44(d)**
  - EACH would like to question how a firm could guarantee that its data is removed/deleted by the CSP. The only possible solution, in our opinion, would be to establish, between the firm and the CSP, a contractual agreement obliging the CSP to delete the data. Similar provisions are already used in the Art 28(3)(g) of GDPR.

Therefore, EACH suggests that the final Guideline 5 require firms to have exit plans in place and review them regularly, but such Guideline should not require firms to test and implement these exit plans. However, when testing exit strategy, we would support the use of a risk-based and proportionate approach. Exit strategies can be reliably estimated based on foundational capabilities such as landing zones in the alternative CSP. Hence, we would suggest that these foundational capabilities be required to be tested for compatibility and the gaps documented.

Guideline 6. Access and audit rights

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

We support the suggested guidance that a firm should ensure that the exercise of the access and audit rights takes into consideration whether the outsourcing is related to a critical or important function, as well as the nature and extent of the risks and impact arising from the cloud outsourcing arrangement on the firm. Nevertheless, as a general remark to **paragraph 51**, we would like to see clarifications on how a firm could effectively extend the scope of any third-party certification scope. In addition, in relation to **point (f) of paragraph 51** we would like to that, currently, some CSPs grant the right to give an expansion of the scope of the certifications or audit reports. However, as of now, contractual arrangements are various: from a customer perspective, it would be helpful if there was a legal requirement to grant these requests.

Guideline 7. Sub-outsourcing

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

Yes, EACH generally agrees with ESMA's approach regarding sub-outsourcing, but EACH would suggest **that the final Guideline 7 is refined so that the requirements only capture**

critical or important elements of critical or important functions (i.e. if immaterial parts of critical or important functions are sub-sourced then those parts should not be subject to these more stringent requirements).

Further, we particularly agree with **point (d) of paragraph 55** and suggest to include a notification about the CPS´s using sub-outsourcing to allow the customer to conduct an internal risk assessment, including the right to object to the sub-outsourcing and the right to terminate if a CSP ignores the objection. With regard to **point (f) of paragraph 58**, see our comment on **point (a) of paragraph 33**.

Guideline 8. Written notification to competent authorities

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

No, EACH does not support ESMA's approach regarding the notification requirements to competent authorities, as Guideline 8 does not seem to take into account already existing notification requirements to regulators on outsourcing arrangements in sector specific legislations.

We note that certain sector specific legislations (e.g. Article 35(1) of the EMIR legislation[4] for central counterparties) already require the regulated entity to obtain approval from their competent authority before outsourcing any major activity linked to risk management. That requirement may also encompass the situation where the outsourcing provider is a CSP, therefore we believe that having a separate notification requirement only for CSPs could lead to a duplication of requirements and to an unnecessary additional administrative burden for firms.

The potential co-existence of the draft guidelines CSP's notification requirement with existing notification or approval requirements for outsourcing of functions could cause misunderstandings in the practical implementation of the requirement. We note that there is a partial overlap between the scope of the notification requirement proposed under Guideline 8, based on a specific definition of 'critical or important function', and the scope of other existing requirements; this could create conflicts across different, but similar/partially overlapping, requirements.

Guideline 9. Supervision of cloud outsourcing arrangements

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

[4] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R2099&from=EN

We encourage competent authorities to monitor and supervise the risks relating to outsourcing of critical or important functions and relevant concentration risks. However, we generally believe that the supervisory authority should first contact the regulated firm, and the regulated firm should deliver information based on requests to the CSP. This approach would reflect the fact that the regulated firm remains responsible for the outsourced function.

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

We would encourage supervisory authorities to harmonise their guidelines on outsourcing / cloud outsourcing arrangements.