|  |
| --- |
| 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. 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](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 | Google Cloud |
| Activity | Non-financial counterparty |
| Are you representing an association? |  |
| Country/Region | Choose an item. |

**Introduction**

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

<ESMA\_COMMENT\_COGL\_1>

**Executive summary**

Google Cloud welcomes the opportunity to respond to the European Securities and Markets Authority (ESMA) Consultation on **the GUIDELINES ON OUTSOURCING TO CLOUD SERVICE PROVIDERS**. We believe that the continuous effort of the European Supervisory Authorities to harmonise regulatory requirements to cloud outsourcing, since the publication of the first European Banking Authority Cloud Outsourcing Recommendations in 2017[[1]](#footnote-2) and further Outsourcing Guidelines in 2019[[2]](#footnote-3), has been absolutely critical to stimulate adoption in the EU financial services sector, remove regulatory uncertainty and further reduce fragmentation. The subsequent Guidelines on outsourcing to cloud service providers by the European Insurance and Occupational Pensions Authority[[3]](#footnote-4) in 2020 have equally made a welcome step clarifying the requirements for the insurance sector, whilst assessing cloud services from the perspective of the great benefit that they bring to the industry. ESMA’s draft guidelines will play an important role in further harmonisation of the requirements for the capital markets, and we value the possibility to provide input into this process.

Google Cloud is committed to the European financial services market, where firms are benefiting from cloud technology in a multitude of ways to understand risk, segment customers, develop new instruments and ultimately offer better and more innovative products to the European consumers. Thanks to the cloud, financial institutions can quickly process large volumes of information, reducing their time to market, and providing more agility and scalability at a lower cost. Capital markets firms can also utilise the cloud to combat fraud and money laundering through artificial intelligence (AI) and machine learning (ML) models. Similarly, cloud-based technologies are being leveraged for firms’ risk-management to determine liquidity and exposure quicker, carry out mark-to-market adjustments and for more effective regulatory reporting. These benefits are fundamental to the industry transformation and need to be accounted for in the forthcoming regulatory guidance.

With this in mind, we believe the following considerations need to be further addressed by the regulator:

1. **Perception of risk and understanding of the cloud security model**: whilst we appreciate the regulator’s focus on risk and fully agree that migration to cloud in the financial sector should be conducted on a risk-based approach, we note that ESMA’s Guidelines are primarily drafted from the perspective of *increased risk* associated with cloud technology and *a perception of the loss of customer control* over their data and infrastructure management. This approach is problematic, in our view, in a number of ways. Firstly, it does not fully reflect the reality of the modern cloud security model where customers benefit from a variety of unique controls allowing them to have transparency over their data and providers’ access to it, with robust security protections - largely by default - that are cost effective, meet international standards, and can fully address customer needs[[4]](#footnote-5). Our **customers remain in control of their data and workloads**, with Google Cloud providing both contractual commitments and technology tools to verify these guarantees[[5]](#footnote-6). Many of Google Cloud security innovations are deeply informed by the requirements of the European financial services customers as well.

Overall the security capabilities that are offered by hyperscale cloud providers have largely surpassed those available on premise, which is broadly recognised by the global financial services industry and regulatory authorities. In fact cloud’s **ability to augment security and reduce the risk** is largely seen today as one of the reasons why regulated industries are accelerating their transition to the cloud[[6]](#footnote-7). From this perspective, we believe that the financial services institutions need to evaluate their cloud strategy with a focus on *risk management and mitigation*, and how their risk management processes can be improved with cloud functionality - not from a starting point of increased security or data privacy risk that is largely implied in the draft ESMA Guidelines (in particular in the Executive Summary).

Secondly, this approach by the regulator may be seen as creating a perception that migration to cloud by securities and capital market firms, supervised by ESMA, is more risky than for those financial services institutions that fall under the EBA and EIOPA guidance, since both EBA and EIOPA have taken a more pro-innovation and benefit-focused approach. Overall, we would recommend that ESMA seek to take a more technology neutral approach.

1. **Approach to mitigation of concentration risk**: as a cloud provider, we understand the regulator concerns over perceived market concentration and systemic risk. We agree it is critical to ensure that proper risk mitigants are in place. For these purposes, it is important to firstly understand and account for **cloud security and resilience capabilities that can overall benefit the financial services industry**, and reduce the risk of single point of failure. Geographic redundancy and multi-regional and multi-zonal deployment of firms’ cloud strategies are fundamental to further ensure operational resilience of their systems.

Secondly, commitment to **the open source and multi-cloud approach** at the industry level is an important lever to mitigate concentration risks. Containerisation and multi-cloud deployment allow customers to build applications once and run them on multiple foreign or domestic infrastructure providers whilst open source platforms can guarantee portability and interoperability in any exit or migration scenario. Google firmly believes in the value of this open source approach that is anchored in [Anthos](https://cloud.google.com/anthos)[[7]](#footnote-8), our hybrid and multi-cloud platform that provides for cloud development and management capabilities across different CSPs and on premise. Adherence to the **open source principles** will be fundamental to the financial sector stability and resilience in the long run, and needs to be endorsed and encouraged by regulators and policymakers.

Finally, a sustainable approach to concentration is only possible with a full understanding of its volume and nature. For these purposes, a **detailed industry register** **of critical or important outsourcing**, as provided for by the draft Guidelines, would be helpful for the regulators to understand the issue at the sector level. We support the suggested approach.

1. **Harmonisation across the existing frameworks**: we note that many ESMA positions (including draft definitions) diverge from the established EBA and EIOPA Guidelines which would inevitably create regulatory fragmentation and challenges in implementation for providers servicing different sub-verticals and firms that fall under the obligations of several frameworks. In particular, the approach to sub-outsourcing defined by ESMA goes beyond the EBA and EIOPA requirements, and appears disproportionate and not consistent with the reality of cloud one-to-many services. We would welcome further effort by the supervisory authorities to harmonise critical definitions and criteria, and are suggesting certain amendments in our detailed response.
2. **Facilitating supervision by competent authorities:** when discussing supervisory risks (paragraph 10), ESMA suggests that cloud providers may be ‘*impairing competent authorities’ ability to perform their supervisory tasks… and may unduly restrict supervisors’ right of access and audit*’. We would strongly challenge this assumption and re-confirm our commitment to transparency and supporting customer compliance with their regulatory requirements. Audit rights are provided for in the EBA and EIOPA outsourcing guidelines, and **Google Cloud consistently facilitates audits by our regulated customers, their supervisory authorities and their appointees**. This commitment is equally acknowledged in our Financial Services contract. Google has facilitated a number of customer audits including, most recently, a pooled audit by the Collaborative Cloud Audit Group (CCAG) and a regulator-led audit in 2019.
3. **Security Guideline:** we caution against defining an overly prescriptive approach to cloud security and controls as currently outlined in the draft Guideline 4. Security capabilities provided by the CSPs, as part of their competitive offering, evolve quickly, and setting a minimum set of requirements or features can rather augment than reduce the security risk. Additionally, approach to security needs to take into consideration cloud multi-tenant and risk-based service models: different controls would be applicable to different customers and their projects based on the individual risk assessment, their business needs and requirements, and in-house expertise. We would recommend that ESMA takes a less prescriptive approach leaving specific security controls designation to customer discretion - consistent with the EBA and EIOPA approach.
4. **Strategy, governance and oversight:** we would like to acknowledge the crucial importance of the firms’ senior leadership involvement in strategy, governance and change management processes to ensure a secure and operational transition to the cloud, and appreciate ESMA’s specific focus and thought leadership in this area. At Google Cloud, we dedicate substantial effort to support customer education and upskilling across different audiences (from expert to executive level), and participate in many designated governance fora consisting of customer and provider leadership which has proved an effective mechanism to oversee the implementation of cloud-driven innovation programmes. We would be happy to share further information and expertise on this focus area should that be of interest to ESMA.

<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>

No comments.

<ESMA\_QUESTION\_COGL\_1>

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

<ESMA\_QUESTION\_COGL\_2>

No. Please see our comments below.

29.h)

**Issue**

The reference to locations where data are “processed” will be problematic if the word “processed” in the Guidelines is given the same meaning as it is under the GDPR.

**Rationale**

“Process” is defined widely in the GDPR. It would include data transport / transit. Specifying the countries through which data transit would be a challenge because – depending on how the firm uses the services – data may (1) transit across networks covering much of the globe, and (2) transit across that global network infrastructure via many different routes.

**Impact**

It would be very impractical for firms to document the countries through which data transit. A requirement to do this would be disproportionate given the lower risks associated with data in transit versus data at rest. This requirement would also be inconsistent with the approach taken to data in transit under the GDPR in the context of international transfers. Without clarification, this paragraph could also lead to competent authorities taking different interpretations. We also note that EIOPA (para 21(e)) and the EBA (para 54(h)) only require documentation of the countries where data are stored. In particular, EIOPA removed the reference to locations where data are processed following their public consultation.

**Suggestion**

We suggest amending the guideline as follows:

“the cloud deployment models and the specific nature of the data to be held and the locations (namely countries) where such data may be stored ~~and processed~~”

29.l.

**Comments**

See our comments above in relation to paragraph 29(h).

In addition, the guideline should recognise that not all sub-outsourcers will have access to, or store, data. Both EIOPA (para 24(f)) and the EBA (para 55(g)) recognise this and only require the location where data is stored if applicable.

**Suggestion**

We suggest amending the guideline as follows:

“where applicable the names of any sub-outsourcer to which material parts of a critical or important function are sub-outsourced, including the countries where the sub-outsourcers are registered, where the service will be performed, and, if applicable, where the data will be stored. ~~and where the data may be processed~~”

<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>

No. Please see our comments below.

33. a) vi.

**Issue**

This paragraph should also refer to whether the conditions for transfer of personal data to a third country under the GDPR are met.

**Rationale**

If personal data are involved, considering whether the conditions for transfer of personal data to a third country under the GDPR are met (and in particular if a recognised compliance mechanism applies to the transfer) is essential to assessing the potential legal risks and compliance issues. As such it will be a critical part of any risk-based approach to consideration of data storage locations in the context of cloud outsourcing.

**Impact**

As drafted, this paragraph does not take the opportunity to achieve further convergence on how firms should assess data storage locations in the context of cloud outsourcing and to align this assessment with the GDPR. This may lead to incomplete risk assessments due to a lack of consideration of valid transfer mechanisms under the GDPR. This could in turn lead to fragmentation as firms consider their obligations for data transfers under both regimes.

**Suggestion**

We suggest amending the guideline as follows:

“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 (in particular, whether the conditions for transfer of personal data to a third country under the GDPR are met) of the countries (within or outside the EU) where the outsourced functions would be provided and where the outsourced data would be stored; in case of sub-outsourcing, the additional risks that may arise if the sub-outsourcer is located in a third country or a different country from the CSP and, in case of a sub-outsourcing chain, any additional risk which may arise, including in relation to the absence of a direct contact between the firm and the sub-outsourcer performing the outsourced function”

33. a) vii.

**Issue**

It is disproportionate to require individual firms to assess possible concentration within the sector.

**Rationale**

Individual firms do not possess the information needed to meaningfully assess concentration within the sector. CSPs are also unable to share confidential information about their relationship with one firm with any other firm. Supervisory authorities, however, will possess this information based on their supervision of all firms and are better placed to perform this assessment.

**Impact**

This could lead to firms attempting to perform a sector assessment without complete information and so arriving at conclusions that - at best - are not meaningful and - at worst - are counter-productive.

**Suggestion**

We suggest amending the guideline as follows:

“possible concentration within the firm (including, where applicable, at the level of its group,) caused by multiple cloud outsourcing arrangements with the same CSP ~~as well as possible concentration within the sector, caused by multiple firms making use of the same CSP or a small group of CSPs~~. When assessing the concentration risk, the firm should take into account all its cloud outsourcing arrangements (and, where applicable, the cloud outsourcing arrangements at the level of its group) with that CSP”

<ESMA\_QUESTION\_COGL\_3>

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

<ESMA\_QUESTION\_COGL\_4>

No. Please see our comments below.

41.f)

See our comments above in relation to paragraph 29(h).

**Suggestion**

We suggest amending the guideline as follows:

“the location(s) (namely countries) where relevant data will be stored ~~and processed~~ (location of data centres), and the conditions to be met, including a requirement to notify the firm if the CSP proposes to change the location(s)”

41.n)

**Issue**

As currently drafted, this paragraph does not expressly limit the access and audit right to the premises, systems etc actually used to provide the outsourced services to the firm. In addition, the reference to “books” is unclear.

**Rationale**

Not all the CSP’s premises, systems etc will necessarily be relevant to the outsourced services and so relevant to any assessment by or on behalf of the outsourcing firm. Any right to access or audit should be expressly limited to those premises, systems etc which are actually used to provide the service to the outsourcing firm.

In addition, we suggest the reference to “books” is replaced with a reference to “information” for consistency with the EBA (para 87(a)) and EIOPA (para 37(m)(i)).

**Impact**

The breadth of this guideline will create uncertainty and friction for both firms and CSPs in contract negotiations and will expose the CSP and its customers to undue operational risk. This will ultimately be a barrier to the use of cloud services.

**Suggestion**

We suggest amending the guideline as follows:

“the requirement for the CSP to grant the firm, its competent authorities and any other person appointed by the firm or the competent authorities the right to access (‘access rights’) and to inspect (‘audit rights’) the relevant information ~~books~~, premises, ~~relevant~~ systems and devicesof the CSP used to provide the cloud outsourcing arrangement to the extent necessary to monitor the CSP’s performance under the cloud outsourcing arrangement and its compliance with the applicable regulatory and contractual requirements, having regard to Guideline 6”

<ESMA\_QUESTION\_COGL\_4>

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

<ESMA\_QUESTION\_COGL\_5>

No. Please see our comments below.

43.

Overall we find ESMA’s requirements to the security approach in certain instances overly prescriptive and not consistent with the nature of cloud outsourcing and security model.

Firstly, it is not advisable to set out a minimum security requirements standard for the firms to apply at the regulatory level, as these security capabilities evolve quickly in response to the technological reality, customer business demands and emerging external threats. Also security features that are developed by different providers are not identical and remain part of their competitive differentiators. Whilst at Google Cloud, we offer many of the capabilities described in the recommendations in principle, including by default, the application of specific controls remains customer choice as in many cases there are tradeoffs between larger customer autonomy and costs, scale of security protections and availability of innovative products.

Approach to *encryption key management*, described in (c) is a good example of a practice that needs to be evaluated and decided on by the customer based on their risk profile, in-house expertise and security capabilities available on premise - as storing encryption keys independently from a CSP, whilst offering certain sovereignty advantages, also creates significant security and other risks[[8]](#footnote-9) which in many cases would outweigh the assumed benefit. Following the risk-based approach, firms should be able to select and adjust their security controls. A one-size-fits-all approach is not effective and is prone to create more risk than it could potentially reduce.

Secondly, many of the specifications on the controls described below are more consistent with the traditional ICT outsourcing and their application on the cloud is fundamentally different, in particular in the context of a shared responsibility model (*eg sections (a) on information security organisation and (b) on access management*), and, in many cases, already more secure by default (*for example the ‘operations and network security’ described in (d) or business continuity and disaster recovery’ in (f)).*

**Suggestion**

Overall, we would recommend that ESMA make this security guideline more consistent with the EBA and EIOPA frameworks by removing the overly prescriptive requirements in paragraph 43.

In particular, we suggest amending the guideline as follows:

“For that purpose, in case of outsourcing of critical or important functions, a firm, if appropriate applying a risk-based approach, should ~~at least~~”

<ESMA\_QUESTION\_COGL\_5>

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

<ESMA\_QUESTION\_COGL\_6>

No. Please see our comments below.

44.c)

**Issue**

It is not clear how this obligation would apply to the IaaS cloud outsourcing context because the customer is in control of retrieval of data from the services.

**Rationale**

Cloud services (and in particular IaaS) are largely automated and controlled by the customer. In particular, the customer decides what data to upload to and retrieve from the services and how and when to do so, and is also in control of (and most familiar with) the applications and products that it builds on the services.

Although the CSP makes tools and functionality available to the customer to retrieve data, the customer operates these tools and functionality and decides when and how to do so.

An unqualified obligation on the CSP to transfer the activity to another service provider or the firm may not work in all cloud outsourcing contexts. Instead, if the service model is such that the CSP could not transfer the activity itself, the obligation on the CSP should be to support the customer to orderly transfer the activity.

**Impact**

As currently drafted, this guideline is not compatible with all cloud service models. Making this a requirement for the agreement will create uncertainty and friction for both firms and CSPrs in contract negotiations. This will ultimately be a barrier to the use of cloud services. We also note the EBA (para 99(c)) and EIOPA (para 55(c)) refer to an obligation to support transfer.

**Suggestion**

We suggest amending the guideline as follows:

“ensure that the cloud outsourcing written agreement includes an obligation for the CSP to support the firm with the orderly transfer of the outsourced function and all the related data from the CSP and any sub-outsourcer to another CSP indicated by the firm or directly to the firm in case the firm activates the exit strategy”

<ESMA\_QUESTION\_COGL\_6>

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

<ESMA\_QUESTION\_COGL\_7>

No. Please see our comments below.

50.f)

**Issue**

It should not be a condition of making use of third-party certifications and audit reports that the firm has the contractual right to request the expansion of their scope.

**Rationale**

In a public cloud context, third-party certifications / reports are a way of providing important information to customers in a scalable way. By performing these assessments against accepted international standards, CSPs ensure they meet the needs of as many customers as possible. This in turn helps to manage the operational burden and risk associated with individual assessments that are required to produce these materials.

It would be disproportionate to expect the CSP to expand the scope of the certifications/reports for a single firm. If each firm makes different requests, this could result in bespoke certifications / reports for each firm. This would necessarily require individualised assessments. As a result, the certifications / reports would lose their relevance to all customers and their effectiveness as a scalable compliance tool.

If the firm believes there is a gap in existing internationally-accepted standards on which the certifications/reports are based or if their own internal risk framework goes beyond internationally-accepted standards, the firm can exercise their access and audit rights to address that gap per paragraph 51(g). In addition, as a long term solution, firms should advocate to the standards body that manages the relevant standard to change it to address any material gaps.

**Impact**

Making this a condition for firms using third party certifications and reports may unduly limit the use of certifications and reports. Alternatively, if CSPs agree to offer this right, there is a real risk that (1) certifications and audit reports will lose their relevance to all customers and will become individualised and bespoke, and (2) providers will have to perform multiple assessments to satisfy each firm’s expanded requirements. In addition, we note that both the EBA and EIOPA make clear that the number and frequency of request for scope modification should be reasonable and legitimate from a risk management perspective.

**Suggestion**

**Option 1 (preferred)**

We suggest deleting this subsection.

**Option 2**

We suggest amending the guideline as follows:

“has the contractual right to request the expansion of the scope of the certifications or audit reports to other relevant systems and controls of the CSP; the number and frequency of such requests for scope modification should be reasonable and legitimate from a risk management perspective”

50.g)

To remain consistent with para 49 of the guidelines, we suggest that ESMA align with EIOPA’s approach at para 43(g) of the EIOPA guidelines.

**Suggestion**

We suggest amending the guideline as follows:

“retains the contractual right to perform individual on-site audits at its discretion with regard to the outsourced function; such right should be exercised in case of specific needs not possible through other types of interactions with the CSP.”

<ESMA\_QUESTION\_COGL\_7>

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

<ESMA\_QUESTION\_COGL\_8>

No. Please see our comments below.

55.d)

**Issue**

A requirement to notify of “any planned sub-outsourcing” is too broad. This is especially the case, if “sub-outsourcing” is defined as “a situation where the CSP further transfers the outsourced function (or a part of that function) to another service provider under an outsourcing arrangement”.

**Rationale**

It would be unhelpful to firms and overly burdensome on CSPs to give advance notice of all sub-outsourcings regardless of whether they affect the CSP’s ability to meet its responsibilities.

**Impact**

This will significantly limit the provider’s ability to update its operations to deliver a better and more efficient service to the firm without a meaningful impact on the firm’s ability to manage the risk associated with cloud outsourcing arrangement. We note that EIOPA (para 50(d)) limits the obligation to informing of “planned significant changes to the sub-contractors or the sub-outsourced services that might affect the ability of the service provider to meet its obligations under the cloud outsourcing agreement”.

**Suggestion**

We suggest amending the guideline as follows:

“include an obligation for the CSP to notify the firm of any planned sub-outsourcing, or material changes thereof, ~~in particular where~~ that might affect the ability of the CSP to meet its obligations under the cloud outsourcing arrangement with the firm. The notification period to be set should allow the firm sufficient time to carry out a risk assessment of the proposed sub-outsourcing or material changes thereof and to object to or explicitly approve them, as indicated in point (e) below”

55.e)

**Issue**

A right of explicit approval or veto for sub-outsourcing is disproportionate in the cloud context.

**Rationale**

A right for a single firm to veto a sub-outsourcer would be overly burdensome from a practical perspective in the context of outsourcing to public cloud service providers. The EBA explicitly recognised this at para 12 of page 6 of the EBA’s final report Recommendations on Outsourcing to Cloud Service Providers.

For example, a public CSP may sub-outsource the physical guarding of one of its data centres to a third party, this sub-outsourcing would apply to all the CSP’s customers using that data centre (this could be millions of different customers). If each customer or even a subset of customers had a right to veto the new sub-outsourcer, the CSP would only be able to proceed if *every single one* of those customers consented / did not object. This would be a huge challenge in practice and would significantly hinder the CSP’s ability to provide services to all its customers.

The absence of a veto right does not expose the firm to undue risk given: (1) the CSP is required to notify the firm in advance of planned changes, and (2) the firm will have the right to terminate under paragraph 55(f). In addition, where a sub-outsourcer is only associated with service delivery at a specific data centre, the firm can also in many cases choose not to use that data centre.

**Impact**

This will be a significant (and in many cases insurmountable) barrier to firms using cloud services. We note that after their public consultation EIOPA (para 50(e)) clarified that the objection right and the termination right were viable alternatives in this scenario and did not need to be additive. To address this point in their Outsourcing Guidelines (which apply beyond cloud outsourcing), the EBA qualified the right to object / explicit approval to scenarios where it is appropriate (para 78(e)) in recognition that in some outsourcing scenarios (e.g. public cloud) it was not appropriate.

**Suggestion**

**Option 1 (preferred)**

We suggest deleting this guideline and amending guideline 55(f) as outlined below.

**Option 2**

We suggest amending the guideline as follows:

“ensure, where appropriate, that the firm has the right to object to the intended sub-outsourcing, or material changes thereof, or that explicit approval is required before the proposed sub-outsourcing or material changes come into effect”

Note that even this change would not be consistent with the EBA approach as their approach in the Outsourcing Guidelines applies beyond cloud outsourcing, whereas the current guidelines only apply to cloud outsourcing.

50.f)

See our comments above in relation to paragraph 29(h).

**Issue**

It is not clear what “undue sub-outsourcing” means.

**Rationale**

Termination is a significant step. If the guidelines will require the firm to obtain a termination right, the exact triggers should be clear. A termination right for “undue sub-outsourcing” is not sufficiently clear.

Beyond the two scenarios the guidelines already list, we cannot see further examples of what could be considered “undue sub-outsourcing". As such, we suggest limiting the termination right to these two scenarios.

**Impact**

This could lead to the inclusion of unclear (and likely unnecessarily broad) termination rights in outsourcing agreements. This does not promote certainty vis-a-vis the outsourcing arrangement. Without clarification, this paragraph could also lead to competent authorities taking different interpretations.

**Suggestion**

We suggest amending the guideline as follows:

“ensure that the firm has the contractual right to terminate the cloud outsourcing arrangement with the CSP in case it objects to the proposed sub-outsourcing or material changes thereof because the sub-outsourcing would materially increase the risk for the firm, and in case ~~of undue sub-outsourcing, i.e. where~~ the CSP proceeds with the sub-outsourcing without notifying the firm or it seriously infringes the conditions of the sub-outsourcing specified in the outsourcing agreement.”

<ESMA\_QUESTION\_COGL\_8>

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

<ESMA\_QUESTION\_COGL\_9>

No. Please see our comments below.

58. e)

See our comments above in relation to paragraph 29(h).

**Suggestion**

We suggest amending the guideline as follows:

“the cloud deployment models and the specific nature of the data to be held by the CSP and the locations (namely countries) where such data may be stored ~~and processed~~”

58. f)

See our comments above in relation to paragraph 29(h).

**Suggestion**

We suggest amending the guideline as follows:

“where applicable, the names of any sub-outsourcer to which material parts of a critical or important function are sub-outsourced, including the country or region where the sub-outsourcers are registered, where the sub-outsourced service will be performed, and, if applicable, where the data will be stored ~~and where the data may be processed~~”

<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>

No response.

<ESMA\_QUESTION\_COGL\_10>

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

<ESMA\_QUESTION\_COGL\_11>

Yes. Please see our comments below on the proposed effective date of the guidelines and the definitions section.

**Section: When?**

If the final report is only expected in Q2 2020 / Q1 2021, then the implementation deadline of 30 June 2021 is too short - especially given the global pandemic. This could potentially be less than 6 months. We note that the EIOPA guidelines only applied 12 months from the final publication date.

**Suggestion**

We suggest that, as a minimum, the guidelines should take effect 12 month from the publication of the final report and that the transitional provisions should be adjusted accordingly.

**Section: Definitions (Cloud Outsourcing)**

**Issue**

The scope of limb (ii) of “cloud outsourcing arrangement” definition is not sufficiently clear and potentially too broad.

**Rationale**

* It is not clear that the arrangement with the third party must qualify as an outsourcing arrangement before it can be assessed as a cloud outsourcing arrangement.
* “Relies on” does not have an established or consistent meaning. It is unclear how this threshold should be applied by firms and competent authorities in practice.

To address the points above, we suggest using the established concept of “sub-outsourcing” to determine whether a service provider should in fact be treated as a CSP.

**Impact**

As currently drafted, limb (ii) will lead to fragmentation. There is also a risk that it could extend the application of the Guidelines beyond the scope of outsourcing.

**Suggestion**

We suggest amending the guideline as follows:

“*Cloud outsourcing arrangement* means an arrangement of any form, including delegation arrangements, between: (i) a firm and a CSP by which that CSP performs a function that would otherwise be undertaken by the firm itself; or (ii) a firm and a third party which is not a CSP by which that third party performs a function that would otherwise be undertaken by the firm itself but only if that third party further thansfers the outsourced function to a CSP under an outsourcing arrangement~~, but which relies on a CSP (for example through a sub-outsourcing chain) to perform a function that would otherwise be undertaken by the firm itself~~. In this case, a reference to a ‘CSP’ in these guidelines should be read as referring to such third party”

In addition, if ESMA has specific scenarios in mind that limb (ii) seeks / does not seek to address, we suggest including them as examples similar to how the EBA provides examples of what should not be considered outsourcing at para 28 of the EBA Guidelines of Outsourcing Arrangements.

**Section: Definitions (Sub-Outsourcing)**

**Issue**

The scope of the “sub-outsourcing” definition is not sufficiently clear and potentially too broad.

**Rationale**

“Part of” does not have an established or consistent meaning. It is unclear what the applicable threshold is and how this should be applied by firms and competent authorities in practice. This language could lead to an arrangement between a CSP and another service provider being considered “sub-outsourcing” even though, if the firm had engaged the service provider directly for the same service, it would not be considered an outsourcing arrangement.

**Impact**

This will lead to fragmentation. There is also a risk that it could disproportionately extend the application of the sub-outsourcing guideline beyond the scope of outsourcing. We also note that the “part of” language is additional to the EBA definition of “sub-outsourcing”.

**Suggestion**

We suggest amending the guideline as follows:

“*Sub-outsourcing* means a situation where the CSP further transfers the outsourced function ~~(or a part of that function)~~ to another service provider under an outsourcing arrangement”

<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>

No response.

<ESMA\_QUESTION\_COGL\_12>

1. <https://eba.europa.eu/regulation-and-policy/internal-governance/recommendations-on-outsourcing-to-cloud-service-providers> [↑](#footnote-ref-2)
2. <https://eba.europa.eu/sites/default/documents/files/documents/10180/2551996/38c80601-f5d7-4855-8ba3-702423665479/EBA%20revised%20Guidelines%20on%20outsourcing%20arrangements.pdf> [↑](#footnote-ref-3)
3. European Insurance and Occupational Pensions Authority (EIOPA), [Guidelines on outsourcing to cloud service providers](https://www.eiopa.europa.eu/content/guidelines-outsourcing-cloud-service-providers_en), 2020 [↑](#footnote-ref-4)
4. <https://cloud.google.com/security/overview/whitepaper> [↑](#footnote-ref-5)
5. <https://cloud.google.com/blog/topics/inside-google-cloud/advancing-customer-control-in-the-cloud> [↑](#footnote-ref-6)
6. See McKinsey, [Making a secure transition to the public cloud](https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/making-a-secure-transition-to-the-public-cloud), 2018

   [↑](#footnote-ref-7)
7. <https://cloud.google.com/anthos> [↑](#footnote-ref-8)
8. <https://cloud.google.com/kms/docs/ekm#considerations> [↑](#footnote-ref-9)