|  |
| --- |
| Response Form to the Consultation Paper  |
| Guidelines on Outsourcing to Cloud Service Providers  |

**Responding to this paper**

ESMA invites comments on all matters in this consultation paper on guidelines on outsourcing to cloud service providers and in particular on the specific questions summarised in Appendix I. Comments are most helpful if they:

* respond to the question stated;
* indicate the specific question to which the comment relates;
* contain a clear rationale; and
* describe any alternatives ESMA should consider.

ESMA will consider all comments received by **01 September 2020.**

All contributions should be submitted online at [www.esma.europa.eu](http://www.esma.europa.eu) under the heading ‘Your input - Consultations’.

**Instructions**

In order to facilitate analysis of responses to the Consultation Paper, respondents are requested to follow the below steps when preparing and submitting their response:

1. Insert your responses to the questions in the Consultation Paper in the present response form.
2. Please do not remove tags of the type <ESMA\_QUESTION\_COGL\_1>. Your response to each question has to be framed by the two tags corresponding to the question.
3. If you do not wish to respond to a given question, please do not delete it but simply leave the text “TYPE YOUR TEXT HERE” between the tags.
4. When you have drafted your response, name your response form according to the following convention: ESMA\_COGL\_nameofrespondent\_RESPONSEFORM. For example, for a respondent named ABCD, the response form would be entitled ESMA\_COGL\_ABCD\_RESPONSEFORM.
5. Upload the form containing your responses, in Word format, to ESMA’s website ([www.esma.europa.eu](http://www.esma.europa.eu) under the heading “Your input – Open consultations” 🡪 “Consultation on Outsourcing to Cloud Service Providers”).

**Publication of responses**

All contributions received will be published following the close of the consultation, unless you request otherwise. A standard confidentiality statement in an email message will not be treated as a request for non-disclosure. A confidential response may be requested from us in accordance with ESMA’s rules on access to documents. We may consult you if we receive such a request. Any decision we make not to disclose the response is reviewable by ESMA’s Board of Appeal and the European Ombudsman.

**Data protection**

Information on data protection can be found at [www.esma.europa.eu](http://www.esma.europa.eu) under the heading [Legal Notice](http://www.esma.europa.eu/legal-notice).

**Who should read this paper**

This paper is primarily of interest to national competent authorities and financial market participants. In particular, this paper is of interest to alternative investment fund managers, depositaries of alternative investment funds, undertakings for collective investment in transferable securities (UCITS) management companies, depositaries of UCITS, central counterparties, trade repositories, investment firms and credit institutions which carry out investment services and activities, data reporting services providers, market operators of trading venues, central securities depositories, credit rating agencies, securitisation repositories and administrators of benchmarks (“firms”), which use cloud services provided by third parties. This paper is also important for cloud service providers, because the draft guidelines seek to ensure that the risks that may arise for firms from the use of cloud services are properly addressed.

**General information about respondent**

|  |  |
| --- | --- |
| Name of the company / organisation | UniCredit |
| Activity | Banking sector |
| Are you representing an association? |[ ]
| Country/Region | Europe |

**Introduction**

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

<ESMA\_COMMENT\_COGL\_1>

**Abbreviations/defined terms:**

**ESMA Guidelines** or **GLs**– ESMA Draft Guidelines on Outsourcing to Cloud Service Providers (ESMA50-164-3342) issued on 3 June 2020

**EBA Guidelines** or **EBA GLs**– Final Report on EBA Guidelines on outsourcing arrangements (EBA/GL/2019/02) issued on 25 February 2019

**CIF** – critical or important functions

<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>

We don’t agree with the suggested approach, due the following reasons:

Definition of outsourcing:

* In aligning to the EBA definition, there should also be the clarification of the following: the definition of outsourcing is independent from the “nature” of the company providing the service (CSP, not CSP, other typologies).
* Sub-outsourcing: as a consequence of the above, also the point (ii) of the proposed definition should not be considered, because a sub outsourcing is, in turn, independent from the typology of the provider.
* Outsourcing is only indirectly defined via the definition of “cloud outsourcing arrangement” as the performance of “a function that would otherwise be undertaken by the firm itself”. Unlike EBA Guidelines (Points 26 et seqq.), the term is not further detailed or delimited, so that, e.g., services not provided on a recurrent or ongoing basis or services usually not performed by firms themselves might be considered outsourcing under ESMA Guidelines, nor are there examples of cloud services which are not to be considered as outsourcing (cf. the list in Point 28 EBA Guidelines). Furthermore, we would recommend to clearly focus on the specifics of the business of the firms in contrast to other industries, e.g. by referring to functions that belong to the core business of firms.

Definition of “critical or important function”:

The proposed definition (page 13) is only partially in line with the EBA Guidelines one. We do not see any advantage in such approach, just a possible root cause of confusion in applying the governance of outsourcing and related additional costs.

All in all, the governance of outsourcing (or even of not outsourcing) agreements involving services provided in cloud mode, should focus on any peculiarity relating to the IT risks arising from the nature of the cloud, while the general governance definition and rules of the outsourcings should fully rely on the EBA Guidelines that already repealed the EBA recommendations on outsourcing to cloud service providers.

Scope of application: With a view to credit institutions, ESMA Guidelines are applicable to “credit institutions when carrying out investment services and activities” (Point 14 and definition “firms” (e) ESMA Guidelines), whereas EBA Guidelines are applicable to credit institutions (Point 9 EBA Guidelines in connection with Article 4(1) point 3, point 1 Regulation (EU) 575/2013) meaning any “undertaking the business of which is to take deposits or other repayable funds from the public and to grant credits for its own account”. Despite this delimitation, outsourcings of credit institutions to CSPs will often affect both scopes, so that a harmonized approach – clarifying also the relationship with other sources and guidelines – will be required in order to simplify the application of regulatory requirements and facilitate a proper risk management. Additionally, a harmonized regulatory framework allows the institutions to better focus on effective risk management, generally provides for a level playing field for the financial industry across the European Union, enhances the negotiation power of firms and institutions towards the CSPs and avoids regulatory arbitrage (see EBA Guidelines, Background, Points 18 and 20, and Section 5.1).

<ESMA\_QUESTION\_COGL\_1>

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

<ESMA\_QUESTION\_COGL\_2>

Yes, mainly due to the following reasons:

* The requirements (art 29) are fully in line with the EBA Guidelines as far as the outsourcing relates to critical functions.
* As regards the not critical ones (art 30), the general principle of proportionality is recalled, that we will tend to interpret in line with the EBA Guidelines requirements for this typology of outsourcings (not critical, article 54).

Outsourcing register (Points 28 et seqq.): While it’s generally appreciated that the information required in the firm’s outsourcing register, especially with a view to non-CIF outsourcings, is more subject to the principle of proportionality, further guideline in this regard (e.g. minimum contents also for non-CIF) might make it easier for firms to meet regulatory expectations and to address information requirements to CSPs, including contractual information obligations related to post-signing changes and changes to sub-outsourcings or new sub-outsourcings by the CSPs.

<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>

Identification and assessment of risks:

* We welcome that the aspects to be considered in the course of the pre-outsourcing due diligence are clearly subject to the principle of proportionality, avoiding a minimum scope that might not fit to the firm and the outsourced function. However, further guideline in this regard might make it easier for firms to meet regulatory expectations and to address information requirements to CSPs.
* With a view to risks related to services being provided or data being stored in third countries, we would appreciate if ESMA could further elaborate on potential risks arising from the cloud service provider (CSP) being based in a third country (esp. non-EU countries) that firms should take into consideration.

More specifically, with regard to 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) of the countries (within or outside the EU) where the outsourced functions would be provided and where the outsourced data would be stored”, including sub-outsourced services (Point 33(a)(vi) ESMA Guidelines) we would like to point out that, in the case of cloud services, this criterion, if deemed relevant in the due diligence of an individual outsourcing, might affect several countries and require procuring extensive external legal opinions. “Legal risk” and “legal system” are concepts that deserve more clarification. <ESMA\_QUESTION\_COGL\_3>

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

<ESMA\_QUESTION\_COGL\_4>

Outsourced function and service levels: With regard to the description of the outsourced function (Point 41(a) ESMA Guidelines) and the agreed service levels (Point 41(i) ESMA Guidelines) we would welcome a clear statement of ESMA with regard to post-signing changes of the services provided by CSPs, in particular with a view to the multi-tenant cloud services which require, from a commercial, technical and strategic perspective, uniform technical development of the cloud solutions, especially with regard to technical updates and security enhancements, requiring changes to the services as agreed in the contract with the CSP’s customers.

Exit strategy: Point 41 ESMA Guidelines does not include a reference to the aspects related to the firm’s exit strategy that need to be reflected in the CIF outsourcing arrangement to enable the firm to effectively exercise its exit strategy, especially with regard to the transfer of data and termination rights (e.g. common standards to be defined at European level).

Resolution: With regard to contractual clauses related to resolution, we suggest ESMA to include and detail requirements related to the resolution scenario, esp. the powers of the resolution authority and the transferability of the cloud outsourcing arrangement, in full alignment with the specifications provided by the SRB with regard to operational continuity in resolution (i.e. adequately documented and resolution-resilient contracts) (March 2020, SRB, “Expectations for Banks”).

Business continuity: From the business continuity perspective, we agree with the proposed approach.

<ESMA\_QUESTION\_COGL\_4>

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

<ESMA\_QUESTION\_COGL\_5>

Yes in general.

While we appreciate that the strong authentication mechanism is a requirement for CSP, further details on type of access to which this requirement has to be applied would help to understand ESMA’s requirements (e.g. only for remote access from CSP personal users). Furthermore, other equivalent requirements (e.g. identity federation between firm and CSP) could be mentioned as an alternative solution.

Regarding the adoption of appropriate key management and encryption solutions to limit the risk of non-authorised access to the encryption keys, further details on applicability cases would help to clarify the requirement (e.g. BYOK / CMEK limited to IaaS / PaaS, considering complexity to implement in SaaS). We suggest also avoiding mentioning encryption of “data in memory” considering the market solutions are not mature enough.

Data location: While we appreciate that the firms can define their approach to data storage and data processing locations in a risk-based manner (Point 43(g) ESMA Guidelines), further details of the aspects to be considered by the firm in the definition of such risk-based approach would help to understand ESMA’s requirements.

Security tests by firms: Regarding the requirement included in the EBA Guidelines on penetration tests (Point 94, 13.2 Security of data and systems) and that cloud services are provided in a standardized way to a wide range of customers using a multi-tenant environment, we doubt that firms should be allowed, or even required, to perform their own tests (e.g., penetration and vulnerability tests) on the CSP’s environment. Therefore we recommend that ESMA clarifies that it does not require the firm to directly perform such tests on CSP’s environment, or if required, only with regard to the activities under the firm’s control (“security in the cloud” as differentiated from the “security of the cloud”).

Business continuity: From the business continuity perspective, we agree with what reported in the point f) in the ESMA Guidelines.

<ESMA\_QUESTION\_COGL\_5>

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

<ESMA\_QUESTION\_COGL\_6>

Transfer of data: With regard to the post-contractual transfer of data (Point 44(c) ESMA Guidelines), ESMA should consider that in some cases, or at least to a certain extent, the firm’s data can be transferred to the firm or a third-party service provider by the firm using standard functionalities of the cloud services. However, we recommend that the ESMA Guidelines clarify that the CSP should be obliged to provide such functionality (or to actively transfer or support the transfer) and that the modalities of such functionalities, transfer or support should not be set forth in a way that hinders or impedes the effective exercise of the firm’s right to retrieve its data after the termination of the outsourcing arrangement. Even in these cases defining e.g., common standards to be adopted by CSP and firms when entering into “cloud outsourcing arrangements” it could be the way to ensure effectiveness of the principles and rules.

Termination rights: We suggest that the “trigger events that could activate the exit strategy” (Point 45(b) ESMA Guidelines) are specified in the ESMA Guidelines, e.g., by giving examples such as the persistent failure of the CSP to comply with the agreed service levels or other key contractual obligations.

Deletion of data: Though with a very limited scope, the CSP might be required by laws or regulations to retain certain data. The identification of the conditions for retaining data could help firms in evaluating such requests from CSPs. Therefore, the requirement to delete data (Point 44(d) ESMA Guidelines) might be further specified in this regard.

Business Continuity:

From the business continuity perspective, with reference to all outsourcing of services that are relevant for critical processes, including those to Cloud Service providers, firms should:

* Check that services (e.g. SLA in case of incident/ service disruption) are aligned to business requirements and insert, within Termination rights clause, also references to BC/DR measures as key obligations;
* Perform (if new services) or review (if existing services) the Business Impact Analysis for what concern the scenario of lack of third party, to consider implications and mitigations in case of severe disruptions that might require the exit strategy (e.g. provider bail out).

In particular, for what concern the second bullet, the responsible business – supported by units in charge of coordinating the outsourcing – has to decide about:

* the full risk acceptance (considering lack of alternatives for the same service – e.g. Swift case – or the unreasonable trade-off between risk and cost for mitigation);
* or the definition of a structured exit strategy (e.g. keeping live an owned alternative platform enabling a seamless migration of flows and core functionalities), including potential alternative procedures for risk mitigation.

<ESMA\_QUESTION\_COGL\_6>

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

<ESMA\_QUESTION\_COGL\_7>

Access and audit right: ESMA states that the firm, the competent authorities and any person appointed by the firm or the competent authorities need to be granted with the right to access and inspect “the books, premises, relevant systems and devices of the CSP 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” (Point 41(n) in Guideline 3 ESMA Guidelines). As the access and audit right is a highly disputed topic in the negotiations with CSPs, we propose to clearly state that the access and audit right needs to be unrestricted, and further detail the scope (business premises including head offices, all devices, systems and networks, all information and data, including financial data, as well as internal and external personnel, advisors and auditors) and ensure that the scope is only limited by the purpose of the audit, i.e. encompasses anything used by the CSP (or its subcontractors) for or in connection with the provision of the services. With regard to the competent authorities and any person appointed by the competent authorities, especially to ensure the effective exercise of the authorities rights if the services are performed in third countries, clarification should be made that the authorities are deemed third-party beneficiaries and, therefore, can directly exercise the contractual access and audit right.

Effective exercise/oversight options: For the correct contract drafting, the clarification that the outsourcing arrangement must not limit the firm’s (and the competent authorities’) effective exercise of the access and audit right (Point 47 ESMA Guidelines) is of utmost importance. Furthermore, it would be advisable to clarify as well (i) that this specifically affects all commercial, technical and organizational stipulations in the outsourcing arrangements (see, with regard to the audit notice, Point 53 ESMA Guidelines) which are extensively used by CSPs in outsourcing arrangements (e.g. notice periods, restrictions of access to certain documents or IT systems, limitations of number of auditors, fees for CSP personnel involved in the audit) and which might be misinterpreted or misused as limitations, and (ii) that the oversight options mentioned in this context refer to, amongst others, the monitoring rights of the firm and the reporting obligations of the CSP (see Point 41(h), (j) ESMA Guidelines).

Risks for environment of CSP: It is correct that the way how the access and audit right is executed should not create inappropriate risks for the CSP’s environment and other clients of the CSP (Point 49 ESMA Guidelines). As this is a common subject of dispute between the firms and the CSPs, it seems advisable to further explain this principle, including clarifying the exceptional nature of such refusal of the firm’s audit request, requiring the CSPs to substantiate the potential risks in detail, defining that it has to be the CSP’s duty to enable alternative audit techniques as requested by the firm which, in the firm’s sole discretion, provide the same level of inspection, and excluding that audits are completely refused by CSPs on the basis of this principle.

Third-party audit certifications, external or internal audit reports of the CSP: With regard to the use of third-party audit certifications, external or internal audit reports of the CSP (Points 50(a), 51, 52 ESMA Guidelines), ESMA generally (i.e. for CIF and non-CIF outsourcings) states that the firm should assess if and to which extent such certifications and audit reports are adequate and sufficient and with regard to CIF outsourcings further defines more detailed prerequisites for the use of such certifications and audit reports, and with this approach differs from the EBA Guidelines (92, 93 EBA Guidelines). In order to avoid a misalignment in the handling of regulatory requirements by the firms, a harmonization of the approaches seems appropriate.

<ESMA\_QUESTION\_COGL\_7>

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

<ESMA\_QUESTION\_COGL\_8>

Requirements for sub-outsourcing: The rules set forth in Point 55 ESMA Guidelines might be misinterpreted in the way that they only apply to CIF outsourcings, whereas at least several of the requirements stipulated therein should as well be implemented in cases of non-CIF outsourcings (e.g., the supervision by the CSP, the back-to-back obligations of the sub-outsourcing provider, the notification obligation and the right to object/terminate). We propose that ESMA clarifies this principle by adjusting the language used in Point 55 ESMA Guidelines accordingly.

Conditions for sub-outsourcing: We understand that the conditions to be complied with in case of sub-outsourcing (Point 55(b) ESMA Guidelines) refer to prerequisites for the sub-outsourcing to be generally permitted (see Point 55(a) ESMA Guidelines), whereas the requirements stated thereafter (i.e. Points 55(c)-(f) ESMA Guidelines) apply nevertheless in all cases of sub-outsourcings.

Supervision by CSP: With regard to the rule set out in Point 55(c) ESMA Guidelines, we propose to clarify that it requires the CSP to (i) oblige its sub-outsourcing providers to comply with the contractual obligations agreed between the firm and the CSP (especially access and audit rights, which may be exercised directly vis-à-vis the sub-outsourcing provider) and (ii) oversee the sub-outsourced services to ensure such compliance.

Notification of planned new sub-outsourcings or changes to existing sub-outsourcings: As such new sub-outsourcings or changes to existing sub-outsourcings become relevant after the signing of the outsourcing arrangement, it is necessary for the firm to define therein the information the CSP has to provide with the notification Point 55(d) ESMA Guidelines). As such information needs to allow the firm to perform a pre-sub-outsourcing analysis and due diligence (see Guideline 2) as well as to comply with its documentation duties (see Points 28 et seqq. ESMA Guidelines), we recommend to expressly state that all information and data required by the firm for these purposes, as defined by the firm in its sole discretion, need to be included in the notification or to be provided thereafter upon request by the firm. We furthermore appreciate that ESMA clarifies that the notification period has to be long enough to allow the firm to carry out a risk assessment and to object to or approve/refuse approval of the sub-outsourcing, it being understood that to safeguard effective exercise of the firm’s rights the approval may not be deemed given at the expiry of the notification period.

Right to object: With regard to the requirements set out in Point 55(e), (f) ESMA Guidelines, certain details should be clarified: (i) We understand that from a securities and markets supervisory perspective the firms should be entitled to object to planned new sub-outsourcings or changes to existing sub-outsourcings, whereas due to the stricter requirements stipulated in Article 28(2) Regulation (EU) 2016/679 (GDPR) in case of personal data processing sub-outsourcings should be subject to the firms’ explicit approval. (ii) Furthermore, we appreciate that the reasons a firm might have to object to or refuse its approval of sub-outsourcings are not pre-defined in the ESMA Guidelines (as they solely depend on the firm’s risk assessment), and we welcome that ESMA, unlike EBA, uses the term “undue sub-outsourcing” to describe sub-outsourcings implemented by the CSP in violation of the outsourcing arrangement (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) and not to describe the reasons for the firm to object. (iii) In case the firm objects to the sub-outsourcing, it is entitled to terminate the outsourcing arrangement (for cause) if the CSP does not remedy the objections, it being understood that the time used for such objection-and-remedy process needs to be included in the notification period. (iv) With regard to the undue sub-outsourcing, and despite the use of “i.e.”, we understand that the cases of undue sub-outsourcing stated in Point 55(f) ESMA Guidelines are meant as examples, and not as an exhaustive list.

Further sub-outsourcings: It might be useful to explicitly state that the rules on sub-outsourcing apply to all stages of outsourcing along the chain of contracts.

<ESMA\_QUESTION\_COGL\_8>

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

<ESMA\_QUESTION\_COGL\_9>

Yes as, in general, nothing in this chapter has been identified as diverging from the general governance

principle.

<ESMA\_QUESTION\_COGL\_9>

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

<ESMA\_QUESTION\_COGL\_10>

Yes, we agree with the suggested approach regarding the supervision of cloud outsourcing arrangements by competent authorities.

<ESMA\_QUESTION\_COGL\_10>

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

<ESMA\_QUESTION\_COGL\_11>

As a general comment/suggestion we see a great opportunity for the banking industry if a clear definition would arise from these GLs relating “lighter” rules/criteria that can be applied in managing some aspects of the contractual obligation relating to the outsourcing (but also not outsourcing) agreements, involving cloud service providers, as described in this document.

See answers to Q1 regarding scope of application and outsourcing definition.

<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>

These GLs might generate additional costs due to possible divergent criteria compared to the EBA GLs 02/2019, referred to the outsourcing scope of application (ref. definition of outsourcing, definition of criticality/importance, sub-outsourcing management).

<ESMA\_QUESTION\_COGL\_12>