30.09.2019

AMICE Response to EIOPA's Consultation on the proposal for Guidelines on outsourcing to cloud service providers

1. Is the scope of application provided appropriate and sufficiently clear?

Yes.

2. Is the set of definitions provided appropriate and sufficiently clear?

No. The definition of "cloud service provider" is not sufficiently clear in the following part "*arrangements with third parties which are not cloud service providers but rely significantly on cloud infrastructure to deliver their services (for example, where the cloud service provider is part of a sub-outsourcing chain) fall within the scope of these Guidelines*". In particular, it is unclear what kind of services (other than cloud services) fall within the scope of the Guidelines. The definition is too broad and includes different types of outsourcing, which are not strictly "cloud" and therefore, shall not fall within the scope of these Guidelines. Besides, the parameter of "*significant reliance on cloud infrastructure*" brings a further element of uncertainty in laying down the perimeter of the Guidelines. To appropriately define the scope of the Guidelines, AMICE suggests deleting the abovementioned reference to third parties, which are not cloud service providers.

Furthermore, the definition of "cloud broker" should be deleted, as the term is not used in the Guidelines. Extending the application of the Guidelines to cloud brokers will create further ambiguity as to who shall be considered responsible for providing the cloud services.

Finally, it is worth considering that cloud computing, as every technology, will change over time. To prevent the Guidelines from becoming obsolete after a short time, technology neutrality should be acknowledged and explicit reference to features and configurations should be avoided (see, amongst others, definitions and requirements around notification, documentation and risk assessment, as well as references to IaaS/PaaS/SaaS, etc.).

3. Is the timeline to implement the Guidelines considered sufficient to ensure a smooth transition from the current operational practices to the ones provided by these Guidelines?

No. AMICE is of the view that the implementation timeline of the Guidelines is not sufficient. The application of the Guidelines from 1 July 2020 requires significant investments and efforts in terms of organisation, IT and advisory services. Therefore, we suggest that the Guidelines shall apply to new cloud outsourcing arrangements after at least one year from the proposed entry into force.

The requirement to review existing cloud outsourcing arrangements with a view to ensuring that these are compliant with the Guidelines from 1 July 2022, imposes significant risks for higher costs due to chargebacks by cloud service providers and/or discontinuation of some cloud outsourcing arrangements as they cannot be renegotiated as required.

4. Is the Guideline on cloud services and outsourcing appropriate and sufficiently clear to enable the distinction between cloud services falling within the scope of outsourcing and the ones not falling within such scope?

No. EIOPA should clarify why outsourcing should be assumed when using cloud services. There are different types of service models for cloud services and the distinction between cloud services falling within the scope of outsourcing and the ones not falling within such scope is open for interpretation. If all arrangements with a cloud service provider as a starting point should be considered as outsourcing, this will entail that any doubts of the distinction for a specific use of cloud service will lead to the service being assumed as outsourcing and potentially lead to higher costs. Therefore, EIOPA should specify in its Guidelines the criteria for cloud services falling outside the scope of outsourcing.

Paragraph 10(a) is not sufficiently clear given that it introduces a new parameter, which is not specific to cloud outsourcing, and is not taken into account by other regulations on outsourcing. It is unclear clear whether that criterion would also apply to other types of outsourcing. Hence, if EIOPA decides to keep a generic definition of cloud outsourcing that is technologically neutral, AMICE suggests deleting paragraph 10(a). Alternatively, EIOPA should clarify whether the performance of the outsourced function on a recurrent or on an on-going basis is a necessary condition to assess the existence of an outsourcing or not.

5a. Is the Guideline on written policy appropriate and sufficiently clear to manage the undertaking's roles, processes and procedures on outsourcing to cloud service providers?

No. Overall, the Guidelines on written policy are in line with Guideline 63 of EIOPA Guidelines on system of governance.

However, it is not clear when insurance undertakings are supposed to update their outsourcing policies. In fact, while addressing the issue of the contractual amendments, the Guidelines do not set any deadline for the necessary adaptations of the outsourcing policy. In particular, it is unclear if the outsourcing policy should be compliant with the Guidelines' provisions by their entry into force or later, at the earliest opportunity (*e.g.* when approving the annual policies). This uncertainty represents an additional reason to postpone the entry into force of the Guidelines, as pointed out above in our answer to question 3.

Paragraphs 16(d) and 16(f) extend the application of the contractual and "exit strategies" requirements to non-material cloud outsourcing arrangements. This is not in line with Article 274 of the Solvency II Delegated Regulation and the principle of proportionality. These should only apply to material outsourcing.

5b. Is the Guideline on written policy consistent to the market best practices on defining the policy for general outsourcing?

No. Not every material outsourcing involves provision of services to policyholders and the options to manage service problems are not necessarily limited to exit, termination and transfer (*i.e.* substitution) of activities. A more open mandate on how to manage critical situations would appear appropriate, *e.g.* by simply requiring "emergency or exit plans" that are proportionate to the nature and scale of the service in question.

6. Is the list of information to be notified to the national supervisory authorities considered appropriate to understand the most significant areas taken into account by the undertakings in their decision-making process?

No. AMICE believes that the notification requirements foreseen in Guideline 4 are quite extensive and detailed.

The requirement to notify a draft version of the outsourcing agreement as stated under paragraph 18 does not exist for general outsourcing contracts. We do not see why there should be a different treatment in the case of cloud outsourcing contracts.

Moreover, it is not always possible to notify the supervisory authority of a draft version of an outsourcing contract prior to the use of the cloud services. In some cases, an agreement is negotiated without being classified as material outsourcing – in particular, in relation to IaaS, PaaS – and it is not before the service is used for hosting of critical services that it is considered as material outsourcing at a later point in time. Such cases should be addressed in the Guidelines.

In relation to paragraph 18(d), it is worth pointing out that extending the notification duty of material outsourcing to all the undertakings within the scope of prudential consolidation seems too burdensome and its actual utility from a supervisory standpoint seems uncertain. In fact, both the outsourcing provisions of Solvency II and EIOPA Guidelines on System of Governance do not embrace non-supervised entities.

Therefore, AMICE suggests limiting the scope of the mentioned notification duty only to the insurance and reinsurance undertakings within the group, whereas excluding "the other undertakings within the scope of the prudential consolidation", as provided in paragraph 18(d).

Besides, in order to monitor the concentration risk, in the case of groups it would be more appropriate to limit the scope of the notification duty to the (re)insurance undertakings that make use of the same cloud service provider.

7a. Would the introduction of a register of all cloud outsourcing arrangement have a significant impact on the current undertakings practices to manage cloud-outsourcing arrangements?

Yes. The introduction of a register of all cloud outsourcing arrangements containing all the information listed under Guideline 5 would have a significant impact on the current practices.

There will be also an impact on the governance surrounding cloud outsourcing, e.g. the undertaking will potentially increase the resources required to ensure compliance with the reporting.

The requirement to introduce a register should only be limited to material outsourcing. Due to the limited materiality and risks associated with non-material functions it does not seem proportionate to extend the obligation to these arrangements.

7b. What can be other approaches to ensure a proper and sound holistic oversight of cloud outsourcing?

As long as the information and data are promptly accessible by the relevant personnel, AMICE believes that the undertakings shall be free to decide where to store the contractual documents and related information.

8. Are the documentation requirements appropriate and sufficiently clear?

No. AMICE is of the view that the documentation requirements should only apply to material outsourcing. For example, paragraph 22 provides that in case of non-material outsourcing the register should include the information referred to in Guideline 4, which also covers exit strategy (paragraph 18(h)). This provision creates confusion considering that the adoption of an exit strategy is only mandatory for material outsourcing (see paragraph 60).

In paragraph 23(i), it is unclear whether EIOPA asks to provide information on the number and skills of the personnel in charge of monitoring the cloud outsourced activity with reference to each single outsourcing agreement or not. AMICE believes it would be sufficient to provide a single comprehensive description of the resources in charge of monitoring the outsourcing agreements and that undertakings should maintain the flexibility to change quickly the number of resources in charge of monitoring each outsourcing agreement. Thus, AMICE suggests specifying the comprehensive nature of the information to be provided according to paragraph 23(i).

9. Taking into account the specific nature of cloud services, it has been opted to use the concept of 'materiality' to clarify, in this context, the concept of a 'critical or important operational function'. Is this approach appropriate and sufficiently clear?

No. The concept of "outsourcing of critical or important operation functions or activities" has been introduced in Article 49 of the Solvency II Directive. Introducing new concepts would be misleading and result in an uneven treatment of different outsourcing options/solutions.

Based on the current wording of Guideline 7, it is not clear if the assessment of material outsourcing includes:

- the identification of "critical or important operational functions" according to EIOPA Guidelines on System of Governance (Guideline 60) and any other material outsourcing according to the factors listed under paragraph 27, or
- if paragraphs 26 and 27 should be read in conjunction, thus, material outsourcing should fulfil the criteria in paragraph 26 as well as in paragraph 27.

10. Is the content of Guideline on risk assessment of cloud outsourcing appropriate and sufficiently clear?

No. The content of Guideline 8 is not sufficiently clear where it states that "*the undertaking should assess the potential impact of material cloud outsourcing both before and after the outsourcing*". AMICE suggests removing the following wording "*both before and after the outsourcing*".

It is also questionable whether performing a cost-benefit analysis along with the risk assessment would be appropriate in this context. This requirement goes beyond the aims of the Guidelines (paragraph 18) and of the Solvency II regulation itself.

Paragraph 30(a) – (g) seem to have overlapping content and should be amended accordingly.

The requirement under paragraph 30(g) (the undertaking should consider political stability and security situation in the country where the cloud service provider is located) can be difficult to comply with.

It would be also difficult to implement the requirement under paragraph 30(h), given that insurance undertakings might have little control over sub-outsourcing by the cloud service provider.

Paragraph 31 seems too prescriptive ("*The risk assessment should be performed before entering into a material cloud outsourcing and on a periodical basis, as defined in the written policy, and, in any case, before renewal of the agreement (if it concerns content and scope)*"). The periodic performance of the risk assessment should be required only if the circumstances suggest a full re-assessment. In most cases, a well-reasoned confirmation that the previous assessment is still valid should suffice.

11. Are the contractual requirements for material outsourcing appropriate and sufficiently clear?

No. Although the contractual requirements provided under the Guidelines are reasonable in theory, it is worth considering that in practice insurance undertakings, in particular SMEs, have very limited negotiating power against cloud service providers. Therefore, it is not obvious that insurance undertakings may be able to enter into agreements in full compliance with the Guidelines. Even if they manage to do so, it would involve long negotiations and considerable efforts with no guarantee that insurance undertakings would manage to effectively enforce their contractual rights.

Therefore, we believe that EIOPA (possibly, in cooperation with EBA) should organise roundtables with cloud service providers in order to achieve a common ground among stakeholders about the contractual requirements on cloud outsourcing. Having the supervisory authorities and representatives of insurance undertakings sitting around the same table to negotiate with the cloud service providers would definitely enable better results in terms of the supervisory objective compared to that within reach of a single insurance undertaking. In fact, a common agreement among stakeholders about the contractual requirements (and, possibly, the agreement on standard contractual clauses) would facilitate the enforcement of such requirements.

Until such a common agreement among stakeholders is reached, AMICE suggests providing a less comprehensive list of contractual requirements.

Paragraph 35 states that the contractual requirements for material outsourcing are "in addition" to the ones defined by Article 274 of the Solvency II Delegated Regulation. Nevertheless, several of the requirements listed under paragraph 35 are already listed under Article 274. Therefore, we recommend that the Guidelines should only include the requirements that are not covered by Article 274.

Some of the sub-points under paragraph 35 seem overly prescriptive and not easily enforceable in practice, such as the requirement to notify the undertaking if the service provider proposes to change the location(s) where the relevant data are stored and processed (paragraph 35(g)). In this regard, it is worth considering that often the data are being processed on a dynamic basis and migrated every few hours between servers in different locations.

Equally burdensome are the requirements on access and audit rights (see our answer to question 13), considering that cloud service providers are reluctant to allow physical access due to issues of confidentiality and privacy of other customers' data.

On the same ground, it is worth considering that the actual testing of the exit plan would bring unnecessary costs and efforts whereas delivering limited benefits considering that undertakings are already required to test business continuity plans. Therefore, AMICE suggests deleting paragraph 35(m).

Moreover, AMICE believes that it is not appropriate to perform due diligence twice on the same service provider. Repeating periodically such due diligence (as implicitly provided by paragraph 16(c)) on the same service provider would not bring any additional value that would justify the efforts and costs of such activity, all the more so since that it is already required that the undertaking should promptly perform a new risk assessment if it becomes aware of significant deficiencies and significant changes of the service provider.

For the same reason, AMICE suggests specifying in paragraph 33 that if the undertaking enters into a second agreement with a certain cloud service provider, the undertaking shall be free to assess whether to perform a second due diligence on the same cloud service provider is appropriate or not.

In this regard, in order to clarify the "one-off" nature of the due diligence on the cloud service provider, AMICE suggests a rewording of paragraph 16(c) as follows: *"(i) risk assessments and due diligence on cloud service providers, including the frequency of the risk assessment*".

12. Are the criteria provided to set the contractual requirements for non-material outsourcing appropriate and sufficiently clear?

No. The requirement under paragraph 38 is already regulated in the GDPR and sets out unclear contractual obligations. Therefore, AMICE suggests deleting it in order to avoid confusion.

13. Are the guideline on access and audit rights appropriate and sufficiently clear?

No. The guideline on access and audit rights sets out detailed and burdensome requirements which would be difficult to apply, in particular vis-à-vis big cloud service providers, such as Amazon, Google and Microsoft.

AMICE welcomes the possibility for undertakings to rely on third-party certifications or third-party internal audit reports but notes the following.

First, it would be difficult to negotiate the right to request "the expansion of scope of the certifications or audit reports to other relevant systems and controls" (paragraph 45(g)) considering that more controls entail a greater cost which is difficult to appropriately quantify *ex ante* and in general terms.

Secondly, AMICE does not deem appropriate that for material cloud outsourcing the undertakings are forbidden to rely solely on third party certifications and reports, as provided under paragraph 46. Although it is important for an undertaking to retain within its personnel the competencies and experience to adequately assess the cloud outsourcing, it is also worth noting that professional third party auditors generally possess a high degree of technical means and experience to properly assess cloud outsourcing. Third party auditors have often more resources and experience in assessing cloud technology than that held by small and medium undertakings and, therefore, leaving the undertakings to handle individually the audit is not the most effective way to achieve the regulatory objective. Therefore, we suggest discarding the provision set forth in paragraph 46.

14. Are the provisions set by this Guideline for security of data and systems appropriate and sufficiently clear?

No. The provisions set by Guideline 12 are too prescriptive and burdensome. AMICE suggests including a specific reference to the principle of proportionality.

The Guidelines should envisage the possibility to delegate to third party auditors the task of monitoring compliance with the requirements of IT security and data protection. As mentioned above, in most cases specialised auditors possess adequate resources (in terms of staff, experience and technological means) to thoroughly assess the cloud service providers, whereas the same do not always apply for small and medium undertakings.

15a. Are the requirements set by these Guidelines and in particular by Guidelines 4 and 5 on notification and documentation requirement sufficiently proportionate? EIOPA welcomes concrete operational examples as to how to ensure that the principle of proportionality is effectively reflected in these guidelines.

No. The principle of proportionality is not sufficiently incorporated into the Guidelines and the undertakings are subject to burdensome requirements for cloud outsourcing that seem disproportionate to the risks stemming from cloud outsourcing.

Regarding Guideline 14, the provision set under paragraph 58 in relation to the concentration risk seems vague and does not take into account the oligopolistic market structure of cloud services, given that only few service providers are able to meet the prescriptive requirements set by the guidelines. Therefore, we suggest discarding the second part of paragraph 58.

It should be clarified that the AMSB should only be updated in case of significant changes or deterioration of the risks in respect of the material outsourcing, so as to avoid information overload without any practical implication.

16. Do you have any comments on the Impact Assessment?

No.