Position Paper

Response to EIOPA consultation on the proposal for Guidelines on outsourcing to cloud service providers

Our reference:	COB-TECH-19-048		
Referring to:	EIOPA consultation paper on the proposal for guidelines on outsourcing to cloud service providers		
Contact person:	Arthur Hilliard, Policy Advisor		
Pages:	19	Transparency Register ID no.:	33213703459-54

Key comments

- Regarding the proposed timeline to apply the guidelines, further flexibility will likely be necessary to facilitate a smooth transition from current operational practices, based on practical industry experience.
- The guidelines should be limited to instances of material outsourcing. Non-material outsourcing to the cloud should fall outside of their scope.
- The definition of material outsourcing should encompass critical and important operational functions or activities only to ensure legal certainty and consistency with the Solvency II Directive (Article 49) and its Delegated Regulation (Article 274 (3)).
- There is a need to distinguish between outsourcing and the purchasing of a service. A key consideration is whether or not the service is an activity that is typically carried out by an insurer as part of its regular insurance business. If the activity/function is linked to the undertaking in its role as an insurer, and concerns services that it could potentially perform itself but for various reasons decides to outsource it to a third party, then this would fall under the definition of outsourcing. However, if it is an activity that any other company could perform (eg payroll, HR), then this should not be regarded as outsourcing and should not fall into the scope of these guidelines, as it would not be considered outsourcing under Solvency II.

General comments

- In some areas, the guidelines go beyond the legal requirements instead of merely concretising them and/or expand the scope of activities and services beyond those covered by the Solvency II Directive. This is particularly evident in formulations such as "In addition to the requirements set out in the Delegated Regulation" (cf. para 35 and 60) and by imposing requirements regardless of the materiality of the outsourcing (eg maintaining a register of all outsourcing to the cloud). The creation of any such new requirements without a legal basis should be avoided. The guidelines should instead focus on particular aspects or characteristics of cloud computing which necessitate a clarification or interpretation of existing requirements.
- The definition by which cloud services are to be considered as material outsourcing (and why) should be clearer with examples and specific guidelines for undertakings and authorities to ensure a level and uniform evaluation.
- Insurance Europe would encourage EIOPA to allow further reliance on the use of third-party certification.

- The principle of proportionality is not sufficiently incorporated into the guidelines – insurance undertakings are subject to burdensome requirements for cloud outsourcing (eg extensive documentation requirements) that seem disproportionate to the risks stemming from cloud outsourcing.
- The relationship between these guidelines and guidelines for other relevant activities (eg GDPR guidelines, EIOPA guidelines on system of governance) should be clearer.
- It should be stressed that all of the burden of complying with these guidelines is borne by the insurer (contractual requirements, audit, monitoring and oversight). However, the enforcement capabilities of individual insurers are limited. In many cases, small and medium-sized insurance companies are faced with BigTechs, which operate neither sectorally nor country-specifically. Cloud providers offer highly standardised products and services. Insurance Europe would strongly encourage EIOPA therefore to engage with cloud service providers to ensure their willingness to adhere to these requirements. In this respect, we also welcome the work being done by the European Commission on the development of standard clauses for cloud computing and believe that this is a mechanism through which EIOPA could ensure cloud providers respect the requirements faced by industry.
- It will be important to consider the implications of outsourcing to cloud service providers based in third countries if there are restrictions on hosting and data access. A high percentage of cloud service providers, providing an important service to European insurers, are based outside of the EU. Insurance Europe therefore encourages a flexible approach to avoid unnecessary complications when complying with EIOPA's guidelines.

Specific comments on guidelines not addressed by the consultation questions

- In guideline 14 paragraph 56(f), we would request the removal of the reference to "independent" verifications as it is not clear how this should be understood other than as another form of external audit that must be performed by insurance undertakings.

- In addition, regarding the requirement in paragraph 56(b) to have "data and information governance systems around the processes performed on the cloud", we see a need for clarification with regard to what exactly these systems should be able to do.

Q1. Is the scope of application provided appropriate and sufficiently clear?

Insurance Europe is of the view that the scope of application of the guidelines is not sufficiently clear or appropriate.

We believe that these guidelines should be limited to instances of material outsourcing, ie the outsourcing of critical or important operational functions or activities, and that non-material outsourcing to the cloud should fall outside of the scope. Only if there are certain risks associated with cloud services that may have a material impact on: a) the insurer's ability to comply with regulatory requirements; or b) its customers, should the cloud services be regarded as outsourcing (ie critical or important functions or activities). The inclusion in these guidelines of requirements for non-material functions would result in burdensome requirements that are disproportionate to the risks stemming from cloud outsourcing.

However, this being said, if it is decided that the guidelines should apply to both material and non-material outsourcing, it is essential to make a better differentiation between the requirements for the outsourcing of critical or important functions or activities and for other non-material outsourcing. This should result in a more

proportionate and simpler framework for the case of non-material outsourcing. For instance, the following guidelines should not apply to non-material outsourcing:

- Guideline 3, paragraph 16 (d) & (f) (written policy on outsourcing to cloud service providers)
- Guideline 5 (documentation requirements (paragraph 22) and inclusion in a register)
- Guideline 11 (access and audit rights)

In order to ensure that the scope of application is sufficiently precise, clear definitions are an absolute necessity (see Q.2). The definition of material outsourcing should encompass critical or important functions or activities only to ensure legal certainty and consistency with the Solvency II Directive (Article 49) and its Delegated Regulation (Article 274 (3)). If cloud outsourcing could be material without being critical or important, more activities would be considered as material, thereby reducing the range of cloud services that would not have to be notified as a material outsourcing. It should be clarified therefore that material outsourcing is not different from the outsourcing of critical or important operational functions or activities.

The guidelines provide criteria for cloud services falling within the scope, which are aligned with the EBA guidelines. However, there are no criteria for cloud services that should not be considered as outsourcing. This is provided in the EBA guidelines (Title II, 3.26). In order to further clarify the scope of application of the guidelines, we would suggest including criteria for cloud services falling outside the scope of outsourcing in the EIOPA guidelines also as this would provide further clarification of the regulatory definition of outsourcing.

Q2. Is the set of definitions provided appropriate and sufficiently clear?

Outsourcing/Material outsourcing:

The definitions of **"outsourcing"** and **"material outsourcing"** lack sufficient clarity. According to the Solvency II Directive, outsourced functions are insurance or reinsurance activities, while in the draft guidelines outsourcing is said to be assumed in the case of cloud services. It is thus unclear whether only insurance or reinsurance functions will be considered as outsourcing or whether every use of a cloud service (such as the backup of employees' data) would be considered as outsourcing. The latter would be inconsistent with existing regulation and additionally lead to a disproportionate burden on insurance companies.

Furthermore, the interplay between Article 49 of the Solvency II Directive and these guidelines leads to uncertainties regarding the difference between material outsourcing and the outsourcing of critical or important operational functions or activities. As further explained below (Q.9), it would then be necessary to clarify if, and in which cases, cloud outsourcing could be a material outsourcing without any critical or important operational function being outsourced, as well as the consequences of such process. However, this would prove problematic not only from the perspective of creating potential uncertainty or inconsistency, but it would also mean that more activities would be considered as material, thereby reducing the range of uses of cloud services that would not have to be notified as a material outsourcing. Insurance Europe is firmly of the view therefore that there should be no distinction between material and critical or important, nor should any new term be introduced that potentially conflicts with the concept of outsourcing of critical or important operational functions or activities. The term "material outsourcing" is undefined in the Level 1 framework. It should be clarified that material outsourcing is not different from outsourcing of critical or important operational functions or activities pursuant to Article 274(3) of the Delegated Regulation. Otherwise, this would introduce different (special) standards for cloud computing compared to general outsourcing.

We also note that the inclusion of a definition of material outsourcing that refers to another section of the guidelines (ie Guideline 7) is not an appropriate approach, nor does it support the aim of the guidelines to provide clarification and transparency.

Public cloud:

To avoid multiple and potentially contradicting definitions of **"public cloud"**, Insurance Europe would propose using existing definitions used by the industry, eg the NIST (National Institute of Standards and Technology) definition: "The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organisation, or some combination of them. It exists on the premises of the cloud provider."[1]

Private cloud:

For the definition of **"private cloud"**, we would propose also using the NIST definition which states that "the cloud infrastructure is provisioned for exclusive use by a single organisation comprising multiple consumers (eg business units). It may be owned, managed, and operated by the organisation, a third party, or some combination of them, and it may exist on or off premises."

Function:

Article 13(29) of the Solvency II Directive defines a **"function"** as special tasks embedded in the system of governance. However, paragraph 6 of the draft guidelines extends the meaning of functions to any processes, services or activities. This goes too far as it neglects the necessary link to insurance-specific activities.

Cloud service provider:

The definition of **"cloud service provider"** also inaccurately suggests equivalence between cloud services and outsourcing transactions (see also Q.1). Furthermore, it is too broad as it would possibly also capture insurers which only offer services supported by cloud technology. Hence, it should be clarified that only the entity which delivers the cloud infrastructure qualifies as a cloud service provider.

Cloud broker:

We suggest deleting the definition of **"cloud broker"** as the term is not used in the guidelines or introduced in the EBA guidelines. Extending the principles in the guidelines to cloud brokers will create complications as to who shall be considered responsible for delivering the cloud services.

Non-material outsourcing:

A definition of **"non-material outsourcing"** might also be helpful (to help distinguish between non-outsourcing, non-material outsourcing and material outsourcing) – non-material outsourcing means an arrangement that falls under the legal definition of outsourcing but that is not material for the undertaking.

[1] See *"The NIST Definition of Cloud Computing"*, Special Publication 800-145.

Q3. 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?

According to the draft guidelines, insurance undertakings should generally review and amend accordingly existing cloud outsourcing arrangements by 1 July 2022. This will likely be unachievable for many firms, considering that these guidelines will require changes to be made to existing cloud arrangements, including re-negotiation of contracts and operational changes. Therefore, further flexibility will likely be necessary to facilitate a smooth transition, a point which seems to be acknowledged by EIOPA in the text. Insurers may, for instance, be signed up to a number of separate cloud outsourcing arrangements, each of which would take time to renegotiate. It may also require the termination of existing agreements and the need to source services through alternative third-party providers. In addition, any modifications or adaptations of existing arrangements require the cooperation and agreement of the respective cloud service providers to any such changes. This can be a lengthy renegotiation process, the timing of which is clearly not in the hands of the insurance undertaking alone.

Insurance Europe would therefore propose that these guidelines should only apply to future contractual agreements with cloud service providers and that existing arrangements should be outside of their scope. As currently drafted, paragraph 8 would interfere with the widely accepted principle of the rule against retroactivity, which prohibits the imposition of ex post facto laws. Retroactive changes to civil law (eg impacting contracts and agreements between private parties) have been found to violate constitutional and economic rights. It would be extremely burdensome to review and amend existing contractual relationships. Therefore, we propose to delete the section referring to the existing arrangements.

If, however, it is decided that the guidelines have to apply also to existing arrangements, then rather than strictly adhering to a specific transitional period, it is crucial to ensure that appropriate adaptability and flexibility exists for cases where a longer period than 2 years would be necessary to ensure a smooth transition to the new arrangements. From practical industry experience, it is very common that licence agreements with cloud providers have a contract period of at least 3 years to secure consistency in the provision of services and a business case that can hold the costs of a tender process and the implementation of the service into the business. Thus, the transitional period for existing contracts should be at least 3 years in order to ensure that these changes can be implemented when the contract is up for renewal and the existing terms expire.

Alongside a transitional period of 3 years, Insurance Europe is supportive of including the provision in paragraph 9 allowing insurance undertakings to inform their supervisory authority if they expect that a longer period would be necessary (ie beyond 3 years) and to agree on an extended timeline for carrying out the review.

Furthermore, cloud outsourcing agreements need to be negotiated at length before being concluded and these guidelines will involve new analysis and strategic processes as well as heavy and costly contractual (re)negotiations. Therefore, the deadline of 1 July 2020 regarding new arrangements is too short for the correct application of final guidelines published at the end of 2019. Thus, these guidelines should apply from 1 January 2022 to every new cloud outsourcing arrangement entered into on or after this date.

Q4. Is the Guideline on cloud service 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?

Insurance Europe agrees that it is crucial to establish whether or not an arrangement with a cloud service provider should fall under the traditional definition of outsourcing. In other words, there is a need to distinguish between outsourcing and the purchasing of a service. An insurance undertaking often does not have a choice between developing and operating its own services or using a third party. In the case of cloud computing, many insurers are effectively purchasing a service which they do not have any capability to develop or perform themselves, eg in the case of IaaS or SaaS applications.

Insurance Europe therefore welcomes the recognition by EIOPA that a key consideration is whether or not the service in question can be considered as an activity that is typically carried out by an insurer as part of its regular insurance business. If the activity/function is linked to the undertaking in its role as an insurer, and concerns services that it could potentially perform itself but for various possible reasons (resources, competencies, finances or strategic decision) decides to outsource it to a third party, then this would fall under the definition of outsourcing. However, if it is a function that any other company could perform (eg payroll systems, HR administration, secure digital mail distribution), then this should not be regarded as outsourcing and should not fall into the scope of these guidelines. Insurance Europe would suggest illustrating the criteria stated in Guideline 1 with examples. For instance, it would be helpful if EIOPA gives more guidance on how to qualify popular and common cloud–based products like Office 365.

Many existing cloud services could not feasibly be performed by an insurer and would not fall within the business activities typically carried out by an insurer. Many solutions on the market today are not offered at all as on-premise solutions and therefore cannot technically be hosted by the company itself, such as Google Analytics, Azure DevOps tool and CtrlPrint, to mention a few examples.

The guidelines provide criteria for cloud services falling within the scope, which are aligned with the EBA guidelines. However, there are no criteria for cloud services that should not be considered as outsourcing. This is provided in the EBA guidelines (Title II, 3.26) and we suggest including criteria for cloud services falling outside the scope of outsourcing in the EIOPA guidelines also as this would provide clarification of the regulatory definition of outsourcing.

For arrangements with a cloud service provider, it is stated that "as a rule, outsourcing should be assumed." We disagree with the statement in the impact assessment that this is a proportionate and sound way to capture and manage the risks related to the use of cloud services. There are many different service models for cloud services and the distinction between cloud services falling within/outside the scope of outsourcing is still very general and provides room 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. Furthermore, by assuming outsourcing as a rule, the assessment process described in paragraph 10 would be almost rendered obsolete. Moreover, it is questionable from a legal point of view to work with assumptions and placing the burden for proving the contrary on the supervised undertakings.

It is also important to recognise the importance of taking into account the materiality of the function outsourced. Only if there are certain risks associated with the cloud services that may have a material impact on a) the insurer's ability to comply with regulatory requirements, or b) its customers, should the cloud services be regarded as outsourcing (ie critical or important functions or activities), and therefore within the scope of these guidelines.

Paragraph 12 should be deleted as the activities performed as part of the internal control system are not particularly related to cloud services. Guidelines should not set out general criteria for the outsourcing classification of cloud services if such criteria are not specific to cloud use. Alternatively, for the avoidance of confusion and in keeping with the overall objective of the guideline, the last paragraph (12) of Guideline 1 should

focus solely on outsourcing to cloud service providers. We would therefore propose, at a minimum, the removal of any reference to outsourcing to non-cloud providers (ie "regardless whether or not those third parties are cloud service providers").

Guideline 1 states that "the undertaking should establish whether an arrangement with a cloud service provider falls under the definition of outsourcing (Article 13(28) of the Solvency II Directive). As a rule, outsourcing should be assumed. Within the assessment, consideration should be given to: a. whether the function (or a part thereof) outsourced is performed on a recurrent or an ongoing basis; and b. whether this function (or part thereof) would normally fall within the scope of functions that would or could normally be performed by the undertaking in the course of its regular business activities, even if the undertaking has not performed this function in the past." Including "or could" goes beyond current Solvency II guidelines (which restricts this to "would") and may be interpreted to extend to different variables. We therefore suggest "or could" is deleted as it creates unnecessary ambiguity.

Q5. 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? Is it consistent with the market best practices on defining the policy for general outsourcing?

Cloud technology is a fast-moving industry where guidelines and control reports tend to be published online just in time for adoption and disclosure. Therefore, a principle-based definition of oversight control as proposed in the guidelines is welcome.

Insurance Europe would stress, however, that the guidelines should focus on particular aspects or characteristics of cloud computing which necessitate a clarification or interpretation of existing requirements. The topics to be addressed in the written policy according to Guideline 3 simply replicate requirements stipulated in Article 274 of the Delegated Regulation. Therefore, Guideline 3 is not only obsolete, but it may also give the impression that existing requirements could be applied in a different way when it comes to cloud outsourcing. Instead of proposing specific points of evaluation for cloud outsourcing, it should leave more room for individual assessments and policies. The specific requirements could be replaced with a more general obligation for the undertaking to ensure that the relevant policies are updated to include any specific requirements for material outsourcing to cloud providers.

Insurance Europe reiterates its view that non-material outsourcing to the cloud should fall outside the scope of these guidelines. This being said, in paragraphs 16(d) and 16(f), the contractual requirements and documenting of exit and termination strategies are extended to non-material cloud outsourcing. This is not in line with Article 274 of the Delegated Regulation, the EIOPA Guidelines on System of Governance or the EBA guidelines and does not comply with the principle of proportionality. Such an approach is disproportionate for non-material outsourcing transactions. The underlying functions or activities are not essential for the continuity of obligations and services to policyholders. We therefore recommend specifying that these paragraphs apply to material outsourcing only, ie critical or important operational functions or activities.

In general, Insurance Europe would question the expectation that the written outsourcing policy needs to be updated in any case. Outsourcing to cloud providers is subject to the same rules and provisions as general outsourcing arrangements. Therefore, the written policy according to Article 274 of the Delegated Regulation is also applicable to outsourcing to the cloud.

There also appears to be some overlap between paragraph 16(b) and 16(c), as both refer to monitoring and management of the outsourcing arrangement. We therefore suggest having one section regulating the governance for the outsourcing arrangements and one section regarding the due diligence of cloud service providers.

With regard to Guideline 2, Insurance Europe would request EIOPA to revisit its position on the role of the undertaking's AMSB. Paragraph 13 implies that the AMSB needs to confirm each material outsourcing transaction. This would exceed the basic prudential requirements. Pursuant to Article 274(3) of the Delegated Regulation, the AMSB only needs to establish a process which ensures compliance with the requirements of the outsourcing of critical or important functions or activities and to confirm the general terms of the outsourcing agreement.

Q6. 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?

Insurance Europe is of the view that the information requested in Guideline 4 exceeds the Level 1 requirements and goes beyond what EIOPA deems necessary with regard to the notification of general outsourcing arrangements. The detailed content of the written notification to the supervisory authority in paragraph 18 is too granular and should instead focus on basic information only, such as name and address of the service provider (parts of (e)), description of scope (a)(d) and the reason for the outsourcing. Current requirements (b), (c), part of (e), (f), (g) and (h) should not form part of this formal notification.

Moreover, Article 49(3) of the Solvency II Directive does not specify the content of the notification. EIOPA's guidelines on system of governance (Guideline 64) solely requires a description of the scope and the rationale for the outsourcing and the service provider's name. Insurance Europe therefore proposes to keep these requirements consistent.

The requirement in paragraph 18(f), in particular the following part: "the cloud service models (for example IaaS/PaaS/SaaS), the cloud infrastructure (ie public/private/hybrid/community)", seems to go into unnecessary detail to provide a level of clarity that is not achievable. The classification of service models is not appropriate anymore and outdated as the boundaries between IaaS, PaaS, SaaS and any other XaaS are blurring. Similarly, the categorization of cloud infrastructure like hybrid or community is open for interpretation and not adding clarity. Furthermore, the requirement to notify the "date of the more recent materiality assessment" seems excessive. Additionally, there does not seem to be any rationale for requiring an assessment of the cloud service provider's level of substitutability.

It might also be worth considering introducing clarification of the following points:

- What is the expected outcome of the notification? Is the supervisor expected to grant an approval to firms to use a cloud service provider or does the regulator only need to be informed about the outsourcing arrangement? We do not believe that such a notification should be used for approval purposes.
- Should firms inform the regulator before or after the outsourcing arrangement is in place? We believe it would be appropriate to do so before. However, we note that paragraph 18 requires that the written notification to the supervisory authority should include a draft version of the outsourcing agreement. This is not requested by EBA in its guidelines, which specify that a draft agreement is only to be transmitted to the supervisor upon specific request. We believe it would be more appropriate to follow

the same approach here, as in practice most undertakings start contract negotiations based on standard general terms and conditions. There is no added value in repeatedly providing this to a supervisor.

- Would firms need to re-submit a notification if there are changes, even minor, to the outsourcing arrangement? We do not believe that re-submitting a notification should be required.

Q7. Would the introduction of a register of all cloud outsourcing arrangements have a significant impact on the current undertakings practices to manage cloud outsourcing arrangements? What can be other approaches to ensure a proper and sound holistic oversight of cloud outsourcing?

The question as to whether or not the introduction of a register of all cloud outsourcing arrangements would have a significant impact on current practices depends on the form the register would take in practice.

If the intention is simply for insurance undertakings to maintain an updated register of all their outsourcing arrangements, then this is a sound governance practice that is already applied by market participants in one form or another. Most undertakings either have a contract management system or a register of all contracts in place, which provides them with the necessary overview and possibility to perform continuous checks on the supplier's compliance, eg with IT security or GDPR. This is therefore something that would form part of the existing internal governance system within insurance undertakings. As such, its overall impact, aside from the additional administrative effort, would hopefully be limited.

However, if the intention would be for the register to be shared on a regular basis with supervisory authorities, or if it would involve additional reporting obligations beyond the notification obligations for material outsourcing, then this would have a more significant impact on current practices. Insurance Europe notes in this respect that paragraph 20 under Guideline 5 states that the register should be made available to the supervisory authority "on request". Irrespective of the lack of legal basis for competent authorities to require such a register, its establishment and maintenance would be very costly. These costs are not justified by any meaningful supervisory purpose as the competent authorities are fully aware of the magnitude of cloud outsourcing arrangements due to their notification by insurance undertakings. In addition, competent authorities are not prevented from requesting further information, if necessary. It should therefore be up to the supervised undertakings to determine how such information requests can be complied with and ensure that information on all cloud arrangements is readily available.

In addition, paragraph 22 makes reference to Guideline 4 and also requires pre-defined minimum information for non-material outsourcing. If the content of Guideline 4 remains as granular as drafted (see comment under Q.6), the reference should be deleted and the content of such an overarching outsourcing register should be defined by insurance undertakings individually. Moreover, paragraph 22 does not seem to follow a risk-based approach, as almost exactly the same requirements are stipulated for material and non-material outsourcing.

Insurance Europe therefore wishes to stress that the guidelines and requirements should be limited to material outsourcing. Due to the limited materiality and risks associated with non-critical or important functions, it does not seem proportionate to extend the obligations to these arrangements. Setting up detailed registration and documentation requirements on non-material outsourcing will only be a hindrance to the undertakings to utilize and benefit from cloud services in a flexible and efficient manner. It should be possible to govern non-material cloud services according to the same internal and external policies and requirements as any other service providers. In any event, we would reiterate our view that non-material outsourcing to the cloud should fall outside of the scope of these guidelines.

If the authorities were provided with the actual assessments on cloud services considered as material outsourcing, it would be possible for the authorities to evaluate if the evaluations were conducted satisfactory and uniformly across the industry and it would be possible for the authorities to issue relevant guidance to undertakings.

It would also be a concern if multiple supervisors/regulators have differing ideas as to what such a register should look like and what information it should contain. It would be preferable to simply have an explanation of the intentions of the supervisor and to leave the implementation as to how this should be achieved entirely to the insurance undertaking (ie principle-based). In the case of large (re)insurance groups with sub-entities, services are outsourced at various levels and re-used within the group. Requiring every sub-entity to maintain an updated list of all outsourced services would create a significant additional effort.

In terms of other possible approaches, one such approach might be to align any requirement for a register of outsourcing contracts with the requirement to keep and maintain data processing agreements with all third-party data processors under the GDPR (Articles 28 and 30). A list of these data processing agreements could be sufficient to provide an overview of outsourcing contracts.

Regarding alternative approaches to ensure a sound holistic oversight of cloud outsourcing, we do not consider cloud outsourcing to be fundamentally different from 'traditional' outsourcing arrangements from a governance perspective. The respective oversight processes have been and are in place (sourcing, legal, data protection, risk, compliance, etc). Given the blurring boundaries of cloud and non-cloud outsourcing arrangements (see Q.6), introducing a separate regime for cloud services would open the door for different interpretations and ultimately increase complexity on both sides – for both the regulator and insurance companies.

In case of any additional requirements for oversight, they should rather be incorporated into the existing frameworks, instead of creating separate processes and registers specifically for this type of outsourcing arrangement.

With regard to paragraph 23(f)-(h), it would be necessary to determine which sub-outsourcing partner should be regarded as "significant". From our point of view, a significant sub-outsourcer is a third party that is providing essential service parts and where the defined service delivery is directly depending on this sub-outsourcer (eg data centre provider).

In paragraph 19, a clear definition should be provided by EIOPA of what constitutes an appropriate period.

EIOPA requires that documentation of past outsourcing arrangements should be maintained within the register. This is not requested in the EBA guidelines. This requirement does not seem proportionate. Negative or positive experiences can play a role in the assessment of a cloud service provider, but this is part of the overall decision-making process. National requirements on filing and archiving exist and should be respected. Nevertheless, including past outsourcing arrangements (non-active) will overload the outsourcing register, without providing any added value.

Q8. Are the documentation requirements appropriate and sufficiently clear?

Insurance Europe is of the view that much of the documentation requirements set out in the draft guidelines are excessive. Moreover, it remains unclear whether the register is related to outsourced functions (paragraph 19)

or cloud outsourcing arrangements (paragraph 21). If EIOPA insists on maintaining all of the listed documentation requirements, the final guidelines would need to clarify the intended scope.

We further suggest removing paragraph 23(d) as cost information should not be relevant to the regulator. This comment is relevant to any section of the guidelines referring to costs (eg paragraph 27(e) etc).

We also suggest the removal of paragraph 23(i) (ie a description of the undertaking monitoring of the cloud outsourced activities), as we fail to see any added value for including such a description in the register. It is too formal and what matters is that which concerns the internal organisation of the undertaking. It should be enough to be able to demonstrate it during a potential supervisor's control.

Currently, the detailed content of the outsourcing register is very granular in nature and should be framed as principles instead. By doing so, each insurance undertaking would have the ability to establish its outsourcing register based on the principle of proportionality, and in consideration of the minimum requirements set out in Guideline 4.

For insurers with undertakings in several countries, potentially different local applications of paragraphs 18 to 23 can also become a challenge. We would therefore prefer that undertakings would not have to assess paragraph 23(h) for every single cloud service provider, but that this is covered when the cloud service provider can show an appropriate certification (eg ISO 27001).

Q9. 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 one of 'critical or important operational function'. Is this approach appropriate and sufficiently clear?

Insurance Europe acknowledges that there is a responsibility on companies to ensure that the relationship with their cloud service provider is appropriately managed and controlled, including assessing which outsourcing activities should be considered as material. However, one of the major issues with regard to assessing the 'materiality' of the cloud outsourcing is the definition of what constitutes critical or important functions or activities. Critical or important, like material, are all highly subjective terms and so it will be difficult for firms to assess whether EIOPA's implicit materiality threshold has been crossed. It is crucial to ensure sufficient flexibility for insurance undertakings in assessing the materiality of their outsourcing arrangements to avoid a situation where almost all uses of cloud services would be considered as critical or important, and therefore result in overly burdensome compliance requirements. This is all the more important in light of the fact that uncertainty exists over what actually constitutes outsourcing and whether the use of the cloud should be considered as a purchased service rather than an outsourced activity.

Insurance Europe understands, however, that EIOPA's use of the term 'material' is to be considered as broader in scope than critical or important operational functions or activities as referred to in Solvency II. This would prove problematic not only from the perspective of creating potential uncertainty or inconsistency, but it would also mean that more activities would be considered as material, thereby reducing the range of uses of cloud services that would not have to be notified as a material outsourcing. We do not see a need to introduce new terms or concepts next to the outsourcing of critical or important operational functions or activities, nor should there be requirements on the materiality assessment that would even exceed the requirements on outsourcing critical or important operational functions or activities (Article 274(3) of the Delegated Regulation):

- Guideline 6 (paragraph 24(c) and (d) transfer requirements related only to outsourced critical or important operational functions or activities to any arrangement with cloud service providers regardless of materiality considerations, or even if it falls under the definition of outsourcing at all.
- With regard to paragraph 27, it is difficult to understand and assess how these criteria should be weighted or prioritised in an assessment as some of the criteria seem to safeguard interests other than outsourcing (such as f and h).
- Moreover, there is no legal reference for requiring the calculation of a cost ratio of cloud expenses to total operational and ICT costs (paragraph 27(e)). The same is true for substitutability assessments of cloud service providers (paragraph 27(g)).
- Paragraph 27(a)(vi) anticipates potential regulation on recovery and resolution planning which will be envisaged in the Solvency II Review but is not yet enacted. We would also add that (iv) and (v) are additional criteria introduced by EIOPA compared with the EBA guidelines and we do not see their added value.

Insurance Europe notes that there are no regulatory shortcomings as regards outsourcing in general, or cloud outsourcing in particular. Guidelines would prove more helpful if EIOPA illustrates examples of critical or important operational functions or activities related to the services of cloud providers. In this context, the assessment of whether cloud services carry or support insurance functions to an extent that creates a certain indispensability of the cloud provider should be taken into account.

The guidelines stipulate that one of the factors to be taken into account when determining the materiality of cloud outsourcing is the protection of personal and non-personal data and the potential impact of a confidentiality breach or other failure. It states in paragraph 27(h) that insurance undertakings should in particular take into consideration data that is business sensitive and/or critical. However, consideration should also be given in this context to the distinction between the permanence and non-permanence of data storage on the cloud provider's server. If data is only transmitted for a very short period of time, eg for the use of computing power, but not permanently stored, this should be classified differently in the materiality assessment than permanent data storage. Moreover, the negative impact in the event of a cloud server failure is significantly lower if only the computing power fails, and consequently processes cannot be executed, than if a server used for data storage fails resulting in a disruption of data access.

In addition, the requirement to take into account the "potential business interconnections" (paragraph 27(f)) will be difficult to fulfil in cases of reinsurance, as the individual customers in the portfolio are not necessarily known. We would therefore suggest deleting this point due to the operational burden in providing such information.

Paragraph 30(h) outlines potential additional risk if a sub-outsourcer is located in a third country, however a high percentage of cloud vendors are themselves outside of the EU.

Q10. Is the content of the Guideline on risk assessment of cloud outsourcing appropriate and sufficiently clear?

Insurance Europe believes that the content is clear but overly prescriptive. In paragraph 30, for example, we suggest that the requirements should not be referred to as "minimum requirements", as there are many different service models for cloud services and the requirements should be adjusted for each arrangement making sure that the requirements are proportionate and fit for purpose. Furthermore, paragraph 30(a)-(g) seems to have overlapping content and should be updated accordingly.

The distinction between the materiality assessment under Guideline 7 and the risk assessment under Guideline 8 is blurred. There are a number of redundancies in terms of the aspects to be considered. These redundancies arise from their separate treatment in the different guidelines. In contrast, we believe that the materiality assessment is an indispensable and integral part of the risk assessment. However, this question does not relate to cloud computing in particular and should be addressed, if considered necessary, in the wider context of general outsourcing transactions.

There are several risk assessment aspects mentioned as new minimum requirements. We would suggest in particular deleting the following ones:

- Paragraph 28: Even if a scenario analysis is only required "where appropriate", it will increase the risk assessment efforts dramatically and moves it in the direction of quantitative tools that require specific knowledge.
- Paragraph 29: As already mentioned, cost information should not form part of regulatory minimum requirements.

For the cost/benefit analysis, a qualitative assessment could be performed but we would not recommend prescribing a quantitative analysis systematically since some of the benefits are more qualitative (eg security).

Crucially, we would also stress that concentration should be assessed at the group level, not at the legal entity level.

In paragraph 30(g), the undertaking must consider the political stability and security situation in the jurisdiction in question. This can be very difficult to gain insight into for an undertaking and could be very difficult to comply with, depending on how it is regulated. It could also make it difficult for undertakings to use providers based outside of the EU.

The requirements in paragraph 30(h) would also be difficult to comply with, as such a level of control over sub-outsourcing providers is difficult, while cloud providers will understandably want to maintain possibilities for sub-outsourcing.

It would also be useful if the guidelines were to include a description of the underlying risks that they are aiming to prevent (see as an example the Australian Prudential Regulation Authority (APRA) "OUTSOURCING INVOLVING CLOUD COMPUTING SERVICES" of 24 September 2018). We also believe that more room for individual policies and use of the general risk frameworks of undertakings would be preferable.

With regard to paragraph 30(h) and as already outlined in earlier comments, it will be necessary to define "significant" sub-outsourcing. The assessment needs to be risk-based (materiality, type of outsourcing, data involved, etc). The main cloud service provider should retain accountability and responsibility for the sub-outsourcer and demonstrate to the undertakings that it performs these duties.

Paragraph 30(i) suggests that an undertaking must carry out an assessment of the concentration risk to cloud service providers with market dominance. However, it may not be easy for a single insurance company to ascertain the market power of different cloud providers, nor to avoid players with market dominance.

Paragraph 31 implies that a comprehensive risk assessment should be carried out before entering into a material cloud agreement in each individual case. It should be clarified that a risk assessment may be aggregated in a general policy. This would reflect the fact that cloud services are highly standardised. It is also stated that the risk assessment should be updated on a periodical basis. Insurance Europe believes that an update is only warranted if the legal or contractual circumstances have changed.

Q11. Are the contractual requirements for material outsourcing appropriate and sufficiently clear?

Article 274(4) of the Delegated Regulation describes the content of the written agreement between the undertaking and the cloud service provider in exhaustive detail. Nonetheless, Guideline 10 (paragraph 35) sets out a number of new requirements that are "in addition" to Article 274 – and several of the requirements are already regulated by Article 274. We would question such an approach and do not see any benefit from the additional requirements. We would instead suggest focusing on guidelines that help clarify existing requirements in the cloud computing context.

Paragraph 35(l): For instance, it is up to the contractual parties to consider insurance coverage for the outsourced activities and whether this issue should be addressed in the outsourcing agreement. Paragraph 35(l) implies that this issue has to be addressed in the insurance contract.

Paragraph 35(g): The requirement under paragraph 35(g) may be very problematic and it is not often part of a contract. Data localisation is an extremely complex question to be answered, particularly in the case of global cloud service provider.

Paragraphs 35(g)(n) and (j): Insurance Europe also notes that paragraph 35(g) and (n) require technical implementations that few cloud service providers are currently able to provide. Similarly, we believe that paragraph 35(j) is very ambitious and detailed, requiring quantitative and qualitative performance targets.

Paragraph 36: Moreover, it is unclear what EIOPA expects when demanding that "special care should be taken of Article 274(4)(h) to (i) of the Delegated Regulation related to the supervision of outsourced functions and activities ('audit and access rights') and termination and exit rights according to Article 274(4)(d) to (e) of the Delegated Regulation". Article 274 does not attribute special emphasis on single requirements set out in paragraph 4 – with regard to the latter, we would like to point out that there is no legal obligation on the cloud service provider to actively assist the exit of the undertaking.

The guidelines should also take into account that there might be more than one document that describes the business relationship, eg associated documentation regarding the data protection or service descriptions. Currently, the expression "written agreement" in guideline 10 suggests one single document that covers everything.

It should also be added that the requirements for material outsourcing should not be perceived as a tick-box exercise and firms should be given some flexibility to negotiate contracts which reflect their circumstances.

Furthermore, a practical element to consider carefully is the extent to which small insurers could realistically gain agreement from mega-vendors on matters such as target SLAs, right to audit etc. Many such cloud providers have commoditised services and contracts which even the larger insurers would struggle to deviate from. This underpins the importance of a proportionate as well as flexible approach and sufficient time to transition to the new requirements.

Finally, Guideline 9 requires undertakings to conduct a due diligence assessment on the cloud service provider. There is no legal foundation for such a requirement. In particular, the requirement cannot be justified with the reference to the obligation to perform a detailed examination to ensure that the potential service provider has the ability, the capacity and any authorisation required by law to deliver the required functions or activities satisfactorily (Article 274(3)(a) of the Delegated Regulation). This examination is not the same as a due diligence assessment as the reference in Article 256(2) of the Delegated Regulation confirms.

Q12. Are the criteria provided to set the contractual requirements for non-material outsourcing appropriate and sufficiently clear?

As previously stated, Insurance Europe wishes to stress that these guidelines should be limited to instances of material outsourcing, ie the outsourcing of critical or important operational functions or activities. We believe that non-material outsourcing to the cloud should fall outside of the scope of the guidelines. However, this being said, if it is decided that the guidelines should apply to both material and non-material outsourcing, it is essential to make a better differentiation between the requirements for the outsourcing of critical or important functions or activities and for other non-material outsourcing.

Paragraph 37 refers to Article 38 of the Solvency II Directive and states that the conditions in that Article should be included in the agreement. This is in our view sufficiently clear. However, for the last sentence of the paragraph, we suggest rephrasing as follows to provide clarity and ensure compliance with Article 38: *"In particular, the undertaking should ensure that the outsourcing agreement or any other contractual arrangement do not impede or limit the supervisory authorities into carrying out their supervisory function and objectives and the effective supervision of outsourced functions and activities."*

In paragraph 38, it is stated that *"In case of non-material outsourcing, clauses within the agreement between the undertaking and a cloud service provider should be written taking into account the type of data stored, managed or processed by the cloud service provider (or, where applicable, its significant sub-outsourcers)."* However, this obligation is relevant for both material and non-material outsourcing of cloud services and is regulated by the GDPR. Also, it is unclear what lies in the obligation "should be written taking into account". We therefore recommend deleting this section as it is already regulated by GDPR and sets out unclear contractual obligations.

Q13. Are the guidelines on access and audit rights appropriate and sufficiently clear?

Insurance Europe recognises the relevance of ensuring the right to audit for insurers. It welcomes therefore the recognition in paragraph 39 of the guidelines that the effective exercise of the right of audit should not be impeded or limited by the outsourcing agreement, as this may be necessary for the insurance undertaking to fulfil all its regulatory obligations.

However, Insurance Europe believes that on-site audits give limited insights into service performance because during an on-site visit, a supervisor for example is likely to see a well-run data centre with server racks, but this will not offer much insight into the provider's compliance with laws and information security standards. In that context, we welcome EIOPA's recommendation to use "third party certifications and third-party or internal audit reports made available by the cloud service provider" (paragraph 44). It should be possible for cloud service providers to obtain certification that verifies certain quality standards and compliance with current regulations, which could also then be listed in a public register serving as an easy-to-access source of information for insurance undertakings.

The guideline sets out very detailed and restrictive requirements for access and audit rights that are applicable to material as well as non-material outsourcing. This could entail a risk that the insurance companies are

prevented from entering into a cloud service agreement due to service providers not wanting to accept the requirements or additional costs.

In conflict with paragraph 44, the rationale behind the requirement in paragraph 45(h) is not clear – retaining the contractual right to perform individual on-site audits. This point requires further guidance on why it is not sufficient to rely on third party certifications and reports. We think that Service Organisation Control (SOC) reports which are widely used within the industry and contain valuable information required to assess and address the risks associated with an outsourced service should be considered sufficient. In any event, we welcome the clarification in paragraph 45(h) that if on-site audits are to be carried out, it is not to be done on a regular basis but only in case of specific needs.

In this context, we also suggest considering direct supervision of cloud providers instead of further industry-specific requirements.

Paragraph 45 (g) provides that undertakings should make use of third-party certifications and third-party or internal audit reports only if they have the contractual right to request the expansion of the scope of the certifications or audit reports to other relevant systems and controls. The right to scope modification is therefore a *sine qua non* condition to make use of a third-party certification and third party or internal audit reports. However, it seems quite unrealistic to believe that every single insurance undertaking could convince a large cloud provider to accept such a condition or to accept it without additional costs. A certification based on international strict standards such as ISO should be enough for these purposes. From our point of view, it should therefore be sufficient for the cloud provider to have standardised certificates and, as a consequence thereof, for each cloud user to evaluate whether further action is needed or not. Generally, due to the complexity of cloud computing, the usage of certifications should be intensified instead of being restricted. In addition, we would also note that the scope of a certification cannot be extended per se. Therefore, in practice this would mean that the undertaking must ask for another type of certification.

It is not entirely clear what the term "significant outsourcers" is supposed to refer to in paragraph 41. Insurance Europe would welcome a clarification that sub-contractors which do not provide important services to the cloud service provider are not within the scope of the undertaking's audit requirements.

Paragraph 43 does not provide helpful guidance as the undertaking's audit requirements remain even if their exercise would create a risk for the cloud service provider. There is little room for contractual agreements on alternative methods. It may help to provide clarification if examples could be provided for what is considered as acceptable "alternative ways to provide a similar level of assurance".

The restrictions on the use of third-party certifications and third party or internal audit reports imposed by paragraph 45 contradict EIOPA's intention to grant relief on the organisational resources of undertakings and cloud service providers. Moreover, paragraph 46 prohibits undertakings from solely relying on these reports "over time", without specifying this period nor providing guidance on the additional measures expected. Given these uncertainties, undertakings and cloud service providers are rather discouraged to consider the use of third-party certifications and third party or internal audit reports. Moreover, it is unclear how insurance companies could "ensure that key systems and controls are covered in future versions of the certification or audit report" (paragraph 45(d)).

Paragraph 46 states that for material cloud outsourcing, the insurance company should not rely solely on third party certifications/pooled audits. However, if EIOPA decides to keep the very detailed and restrictive requirements in paragraph 45, we do not agree with this restriction as the third-party certifications/pooled audits will provide a very thorough level of assurance. It would be helpful in any case if EIOPA would provide some clarification on instances where third-party certification may not be appropriate.

Physical on-site access to the facilities of cloud providers, as suggested in paragraph 47, does not enhance the audit capability of an undertaking. This is because physical access to IT infrastructure does not provide the ability to verify which data is being managed on the devices. Generally, relevant certifications of the cloud provider (eg ISO 27001, ISO 27017 or ISO 27018) should be sufficient to demonstrate that sound practices are being applied, without the need for further assessments.

Insurance Europe would welcome the publication by EIOPA of an opinion on minimum requirements for service providers in terms of quality certifications.

In the case of non-material outsourcing in particular – assuming that the guidelines would apply in such a case – a local on-site visit is not feasible. The form of audit should be chosen depending on the identified risks and criticalities with regard to respective data and processes.

Q14. Are the provisions set by this Guideline for security of data and systems appropriate and sufficiently clear?

Insurance Europe agrees that there is a need to ensure that cloud service providers comply with appropriate IT security and data protection standards. The quality of the service delivered by the cloud provider is dependent on its ability to appropriately protect the confidentiality, integrity and availability of the data and of the systems and processes used to process, transfer or store this data.

Insurance Europe is of the view therefore that it would be useful to work on a common European standard for outsourcing that covers both the demands of any relevant European guidelines and the General Data Protection Regulation (GDPR). This could take the form of an ISO standard for cloud providers, or alternatively could be some form of industry-agreed standard. This would allow the cloud service provider to document upfront that the storage and handling of the data of a financial services company using its cloud solution is carried out in a sufficiently safe and secure environment. It would therefore minimise the companies' extensive work on documenting, conducting risk analyses and assessing the supplier prior to the conclusion of an outsourcing agreement. It would also lessen the need for substantial contractual negotiations in order to comply with any guidelines and rules on outsourcing.

It should also be added, however, that there is often a lack of awareness or misconceptions regarding the security and safety of data in the cloud. Raising regulatory awareness of the benefits and security offered by the public cloud is also necessary. While the cloud may have different considerations compared with traditional data centres, this does not mean that it is in any way less secure. In fact, given providers' many years of experience and specialised staff, security in the cloud is highly sophisticated and often superior to that which could be maintained by an individual entity. For many companies, leveraging the size and scale of large cloud providers might actually be a part of a more efficient overall security strategy.

As regards paragraph 50(f), a data residency policy in the context of the public cloud may prove problematic. With a global data centre setup, customers can choose to deploy to multiple locations provided by the cloud provider. The purpose of such a policy is not clear therefore. In any case, any requirements regarding a data residency policy will form part of the agreement or service description, so it should be made clear that this policy is not a standalone document.

Paragraph 50(g) constitutes an obligation of ongoing monitoring of compliance with data protection requirements. In contrast, the GDPR only requires the capacity to provide evidence to verify that protection requirements are met. Therefore, the wording of Guideline 12 and the GDPR should be aligned.

In addition, it should be made clear in paragraph 50(g) that in the case of sub-outsourcing the main cloud provider is – from the operative and formal point of view – responsible for steering and controlling its associated third parties. Moreover, the outsourcing company as "risk owner" has to ensure that the main cloud provider also controls its associated third parties adequately. We would suggest making clear that the outsourcing company is not responsible to audit every sub-outsourcing party individually but rather audits the main cloud provider including its third-party management.

As an overall comment on the guideline, we suggest specifying that the principle of proportionality should be taken into account in the assessment of which appropriate IT security requirements should be included in the outsourcing agreement. We find it too burdensome for insurance companies that the requirements for the security of data and systems are applicable to outsourcing of cloud services in general and not only material outsourcing. The requirements for security of data and systems are very detailed and prescriptive and we suggest having a more principle-based approach to the necessary IT security requirements that depends on the output of the risk assessment.

The provisions are wide-ranging and may be appropriate for outsourcing of some cloud services but seem excessive for outsourcing of minor services with low availability requirements. It would be appropriate to refer to a risk-based approach, where the organisation can focus resources on more critical services.

We would propose rephrasing paragraph 50 as follows "…*on the basis of the risk assessment performed in accordance with Guideline 8, taking into account the materiality of the outsourcing and the nature and extent of the risk and impact on the undertaking from the cloud outsourcing arrangements, should*:"

Q15. Are the requirements set by these Guidelines and in particular by Guidelines 4 and 5 on notification and documentation requirements sufficiently proportionate? EIOPA welcomes concrete operational examples as to how to ensure that the principle of proportionality is effectively reflected in these Guidelines.

Insurance Europe is of the view that some of the guidelines have been extended to outsourcing arrangements that are not considered critical or important, and this does not take into account the principle of proportionality. For some sections, there is an explicit reference to the fact that the principle of proportionality should be taken into account. To provide more clarification on how and where to apply the principle, we suggest to either generally elaborate on the principle for outsourcing of cloud services or incorporate the application of the principle into further specific guidelines.

Maintaining the possibility for insurance undertakings to define their own way of documenting their cloud arrangements that are in place would be a better way to ensure a flexible and more proportionate use of cloud services.

Most of the guidelines address aspects which are considered to be in the best interest of the insurance undertaking before entering into cloud service agreements, but they also introduce needless bureaucracy and partly new obligations which even exceed Level 1 requirements. This applies in particular to Guidelines 4 and 5.

We do not see an operational way to orderly reflect the proportionality principle here except by waiving certain requirements.

Certain other guidelines, while reasonable, do not meet the realities of the business environment. For instance, Guideline 13 is unlikely to be enforceable as cloud service providers operate worldwide with sub-contractors. In Guideline 15, the mentioned testing of exit plans "where appropriate", should – if at all – only cover elements on the side of the affected insurance companies.

Insurance Europe also wishes to highlight the following:

- Paragraph 53: in relation to sub-outsourcing, we suggest that the cloud provider retains full "accountability" in addition to "responsibility" and would ask that a reference to accountability is included in the paragraph.
- Paragraph 60(a): clarification is needed on what is meant by "sufficiently tested", ie is there an expected level of detail the testing should meet?

One observation regarding the draft guidelines is that it may be worth introducing direct regulation of the cloud service providers in the long run instead of delegating responsibilities which serve the public good to insurance undertakings.

We also note in the context of the general wording of these draft guidelines that the word "should" is best interpreted as a strong recommendation rather than an obligation ("must") to allow for a better application of proportionality.

Q16. Do you have any comments on the Impact Assessment?

EIOPA may wish to consider the option of including cloud providers offering services to supervised entities directly into the scope of the regulatory framework, as it may simplify compliance with regulatory requirements.

In addition, options for the EU-wide development of standards and certificates, for example by ENISA, should be explored.

We would also welcome if EIOPA would thoroughly investigate and make use of synergy potentials, particularly with regard to the considerable set of different documentation based on the same assessment.