EIOPA-BoS-20-002
31 01 2020

Final Report on public consultation No. 19/270 on Guidelines on outsourcing to cloud service providers

Table of Contents

1. Executive summary

Introduction

1. Under Article 16 of Regulation (EU) No 1094/2010, EIOPA may issue guidelines and recommendations addressed to competent authorities or financial institutions with a view to establishing consistent, efficient and effective supervisory practices, and to ensuring the common, uniform and consistent application of Union law. Before adoption of the final guidelines EIOPA shall, where appropriate, conduct open public consultations and analyse their potential costs and benefits.
2. On 1 July 2019, EIOPA launched a public consultation on the draft Guidelines on outsourcing to cloud service providers. The consultation paper, which was adopted by the Board of Supervisors, is also published on EIOPA's website[1].
3. EIOPA identified the need to develop these specific guidance on outsourcing to cloud service providers in the context of the analysis performed to answer the European Commission FinTech Action plan (COM(2018) 109 final) and following discussions and exchanges with stakeholders[2].
4. Cloud services are a combination of a business and delivery models that enable on-demand access to a shared pool of resources such as applications, servers, storage and network security. The services are, typically, delivered in the form of Software as a Service ("SaaS"), Platform as a Service ("PaaS") and Infrastructure as a Service ("IaaS").
5. Compared with more traditional forms of outsourcing offering dedicated solutions to clients, cloud outsourcing services are more standardised, which allows the services to be provided to a larger number of different customers in a highly automated manner and on a larger scale. Although cloud services can offer a number of advantages, such as economies of scale, flexibility, operational efficiencies and cost-effectiveness, they also raise challenges in terms of data protection and location, security issues and concentration risk, not only from the point of view of individual undertakings but also at industry level, as large suppliers of cloud services can become a single point of failure when many undertakings rely on them.
6. EIOPA acknowledges that, compared to traditional information and communication technology ("ICT") systems, in cloud based systems the cloud service provider and cloud customer share the control of a cloud system's resources. The cloud's different service models affect their control over the computational resources and, thus, what can be done in cloud based systems. This means that, also from a security and control perspective, the cloud provider and the cloud customer might share responsibilities. As a general principle, cloud customers are always responsible for what they do in the cloud and the cloud service providers are responsible for the cloud. Nonetheless, insurance and reinsurance undertakings remain responsible for complying with all their regulatory obligations when they outsource, including to cloud service providers. This includes an expectation that undertakings inform their cloud service providers that they are subject to these guidelines.
7. The use of cloud outsourcing is a practice common to all financial undertakings and not only to insurance and reinsurance undertakings. Moreover, the main risks associated to this practice are similar across sectors. Acknowledging this, and recognising the potential risks of regulatory fragmentation in this area, EIOPA has considered the most recent guidance published by the European Banking Authority (EBA) on this field: the EBA Guidelines on outsourcing arrangements

[1] The consultation paper can be obtained here

[2] The report published by EIOPA as answer to the European Commission FinTech Action plan can be obtained here

(EBA/GL/2019/02) which have incorporated the EBA Recommendations on outsourcing to cloud service providers (EBA/REC/2017/03).

8. The aim of these Guidelines is to:

   (a) provide clarification and transparency to market participants avoiding potential regulatory arbitrages;

   (b) foster supervisory convergence regarding the expectations and processes applicable in relation to cloud outsourcing.

Content

This final report sets out the final text of the EIOPA Guidelines on outsourcing to cloud service providers, including the feedback statement to the public consultation, the final impact assessment and the resolution of non-confidential comments provided by the stakeholders during the public consultation.

Next steps

In accordance with Article 16 of Regulation (EU) No 1094/2010, within 2 months of the issuance of these Guidelines, each competent authority shall confirm if it complies or intends to comply with these Guidelines. In the event that a competent authority does not comply or does not intend to comply, it shall inform EIOPA, stating the reasons for non-compliance.

EIOPA will publish the fact that a competent authority does not comply or does not intend to comply with these Guidelines. The reasons for non-compliance may also be decided on a case-by-case basis to be published by EIOPA. The competent authority will receive advanced notice of such publication.

EIOPA will, in its annual report, inform the European Parliament, the Council and the European Commission of the guidelines issued, stating which competent authority has not complied with them, and outlining how EIOPA intends to ensure that concerned competent authorities follow its guidelines in the future.

2. Feedback statement

Introduction

EIOPA received 28 contributions by several stakeholders (10 (re)insurance undertakings, 10 industry associations, 3 cloud service providers and 5 other institutions) to the public consultation concerning the draft Guidelines on outsourcing to cloud service providers. About half of the stakeholders have provided confidential feedback.

The consultation paper included 16 questions encompassing several areas of the Guidelines. The responses received were very detailed and covered extensively all the Guidelines. Grouping the responses per subject covered, the total number of comments received was more than 500.

The responses received have provided important feedback to EIOPA in preparing the final version of these Guidelines. EIOPA considered carefully all the comments made. A summary of the main comments received and EIOPA's responses to them can be found in the sections below. The full list of all the non-confidential comments provided and EIOPA's corresponding responses can be found in Annex III of this Final Report.

The areas of the Guidelines with the most significant number of comments were: scoping, definitions (including the replacement of "material" with "critical or important") application of the principle of proportionality in relation to a number of areas, implementation timelines, notification and documentation requirements, risk assessment, access and audit rights and security of data and systems.

General comments

Several stakeholders requested EIOPA to further strengthen the principle of proportionality by focusing the requirements of the Guidelines only on outsourcing of critical or important operational functions or activities to cloud service providers and by the removal of the documentation requirements. On the other hand, several comments aimed for a better harmonisation of the requirements set by these Guidelines across the European financial sectors. Some stakeholders made reference to a possible definition of a European supervisory framework for direct oversight of cloud service providers and development of common standards (e.g. standard contractual clauses or ISO standards).

Acknowledging that the scope of these Guidelines (i.e. outsourcing to cloud service providers) is narrower than the EBA Guidelines on outsourcing and aiming at embedding the principle of proportionality and a risk-based approach on their implementation, EIOPA has streamlined the contents of the Guidelines, mainly focusing on outsourcing of critical or important operational functions or activities to cloud service providers. These changes have been done to emphasize EIOPA's willingness to focus on substance over form.
Moreover, in order to foster the harmonisation of the practice related to cloud outsourcing across sectors, EIOPA reviewed the wording of several Guidelines to ensure its alignment (where possible) to the requirements set by the EBA.
On the suggestion to develop a European supervisory framework for the direct oversight of cloud service providers, EIOPA refers to the Joint Advice of the European Supervisory

Authorities to the European Commission on the need for legislative improvements relating to ICT risk management requirements in the EU financial sector[3]. While on the point related to common standards, EIOPA refers to the European Commission's work to develop a set of standardised contractual clauses as part of the FinTech Action Plan and the initiative to develop a SWIPO code of conduct[4].

Scope of application

Several stakeholders requested EIOPA to clarify how the Guidelines should be applied in the context of groups. With particular reference to the application of the Guidelines at solo level by group subsidiaries belonging to other financial sectors, for example, investment management companies licensed under the Undertakings for Collective Investments in Transferrable Securities Directive ("UCITS") or Alternative Investment Fund Management Directive ("AIFMD") – and in case of intra-group outsourcing.

EIOPA welcomed the comments and clarified both points in the final text of the Guidelines.

Definitions

The area of definitions is one of the most commented in the public consultation. The comments mainly focused on the removal of redundant and unclear definitions including the concept of "material function".

The table below is a summary of the comments received on the definitions and EIOPA's resolutions in the final text of the Guidelines.

Definition	Summary of the main comments	Resolution of the comment
Cloud broker	Delete the definition	Agreed. The definition has been deleted
Cloud service providers	Clarify the definition	Agreed. The definition has been clarified
Cloud services	Align the definition to the one provided in Article 4(19) of the Network and Information Security Directive	Disagree. The definition has been kept aligned to the one used in the EBA Guidelines on outsourcing
Function	Delete the definition	Agreed. The definition has been deleted
Material outsourcing	Delete the definition and use the concept of critical or important operational functions or activities	Agreed. The definition has been deleted and the changes have been also reflected throughout all the Guidelines
Private cloud	Clarify the definitions	Disagree. The definitions have been kept aligned to the one used in the EBA Guidelines on outsourcing
Public cloud		
Hybrid cloud		
Significant sub-outsourcing	Delete the definition	Agreed. The definition has been deleted

[3] The joint advice can be obtained at this link.

[4] Additional information on the SWIPO code of conduct initiative can be obtained at this link.

Date of application

Several respondents considered the time granted to implement the Guidelines as too stringent with particular reference to the provisions related to the review of existing arrangements (some stakeholders proposed to grandfather the existing arrangements or to review them on a best effort basis). Further comments suggested to better specify the timeline to update (where needed) the undertaking's policies and internal processes in accordance with the Guidelines.

As response to these comments, EIOPA has moved the date of application from 1 July 2020 to 1 January 2021 and has prolonged the period for reviewing the existing arrangements from 1 July 2022 to 31 December 2022. Furthermore, the due date to perform the update (where needed) to the undertaking's policies and internal processes has been set to 1 January 2021.

On the proposal to grandfather existing obligations, EIOPA has not agreed with the proposal. However, in order to make the Guidelines more proportionate, a principle of risk-based review has been introduced (i.e. only contract related to critical and important operational functions or activities should be amended). Furthermore, the flexibility clause contained in the draft version of the Guidelines has been kept.

Cloud services and outsourcing

Almost all the respondents requested EIOPA to eliminate the assumption that all arrangements with cloud service providers should, as a rule, be assumed as outsourcing. Moreover, a number of respondents asked to better clarify the content of the Guideline by including examples of cloud arrangements not considered outsourcing.

EIOPA agreed with the requests from the respondents and eliminated the sentence "as a rule outsourcing should be assumed" from Guideline 1 "Cloud services and outsourcing".

On the request to include examples, considering that some examples have already been included in the explanatory text of the EIOPA Guidelines on System of Governance, EIOPA has decided to not include in the Guidelines examples of cloud services that are not to be considered as outsourcing.

General principles of governance

Few respondents suggested to clarify the role of the administrative, management or supervisory body ("AMSB") in accordance with the requirements set by Article 274 of Commission Delegated Regulation (EU) No 2015/35.

EIOPA agreed with the comments and clarified the role of the AMSB in line with the above-mentioned regulatory requirements.

Update of the outsourcing written policy

Several comments were made on Guideline 3 mainly requesting the requirements to update the undertaking's internal policies to be less prescriptive and more focused on cloud outsourcing of critical or important operational functions or activities. Some of the

respondents requested EIOPA to delete the Guideline as considered of scarce benefit since the requirements set by Guideline 3 are already embedded in current provisions on outsourcing.

EIOPA has decided to keep Guideline 3 with clarification of its application. For this reason, as the Solvency II principles on outsourcing are still valid for cloud outsourcing, with reference to the update of internal policies and procedures, multiple solutions are at disposal for undertakings:

(i) development of a dedicated cloud outsourcing policy;
(ii) complement the existing outsourcing policy and the other relevant internal policies (for example, the information security policy) to take into account the specificities of outsourcing to cloud service providers;
(iii) if the undertaking's current policies cover the elements described in these Guidelines, there is no need to update.

EIOPA has also enhanced the focus of the requirements toward the outsourcing of critical or important functions or activities to cloud service providers.

Written notification to the supervisory authorities

Overall, most of the comments mainly focused on (i) the removal of the requirement to submit a draft contract as part of the written notification prior to outsourcing a critical or important operational function or activity to a cloud service provider; (ii) the reduction of the number of items to be notified to the supervisory authorities.

The content of Guideline 4 "Written notification to the supervisory authorities" which is related only to outsourcing of critical or important operational functions or activities has been streamlined by (a) removing the requirement to present a draft copy of the outsourcing agreement; and (b) aligning the requirements to the EBA's requirements set by paragraph 54 of the EBA Guidelines on outsourcing.

Documentation requirements

Overall, Guideline 5 "Documentation requirements" was the most commented of the entire public consultation. The main comments focus on: (i) removal of the requirement to keep a register of cloud outsourcing arrangements; (ii) application of the Guideline only in case of outsourcing of critical or important operational functions or activities.

EIOPA has streamlined the content of Guideline 5 in order to make it more principle and risk based (i.e. no specific provisions related to keep a register but to record information). Moreover, EIOPA has defined a minimum set of information to be recorded only for outsourcing arrangements related to critical or important operational functions or activities outsourced to cloud service providers. This set of information is aligned to the one required by the EBA Guidelines on outsourcing. For outsourcing arrangement with cloud service providers of non-critical or non-important operational functions or activities, the level of detail of the information to be recorded should be determined by the undertakings on a risk-based approach.
EIOPA acknowledges that the changes made are a major departure from the requirements set by the EBA Guidelines on outsourcing, which requires firms to maintain a register on all outsourcing arrangements. This decision was taken under the

assumption that a broader and more comprehensive discussion on how document outsourcing arrangements will be undertaken when reviewing the System of Governance Guidelines.

Materiality assessment

The main comment provided by almost all respondents with respect to Guideline 7 is related to the risk of confusion between the term "material outsourcing" (used in the draft version of the Guidelines issued for public consultation) and the term "outsourcing of critical or important operational functions and activities" (used in Guideline 60 of EIOPA Guidelines on System of Governance). Other comments made on this Guideline asked EIOPA to reduce the number of factors to be taken into account while performing the assessment.

In the draft version of the Guidelines issued for public consultation, EIOPA opted for introducing the definition of "material outsourcing" with the aim to have a more risk-based approach in the assessment of cloud outsourcing contracts taking into account the specificities of these type of services. EIOPA was aware of the risks of potential confusion between the new term and the well-established concept of "critical or important operational functions or activities" and for this reason, EIOPA asked a specific question in the consultation paper on this point.

On the basis of the feedback received and bearing in mind that one of the main purposes of these Guidelines is to provide clarity to the market participants, EIOPA decided to withdraw the use of the term "material outsourcing" and replace it with the term "critical or important operational function and activity". As a consequence, EIOPA changed the title of the Guideline from "Materiality assessment" to "Assessment of critical or important operational functions and activities."

In addition to the above-mentioned change, EIOPA has reviewed and streamlined the content of Guideline 7 striving to further align the factors to be taken into account when performing the assessment to the ones requested by paragraph 31 of the EBA Guidelines on outsourcing.

Risk assessment

Several comments were made on Guideline 8 "Risk assessment" mostly aiming at increasing the level of proportionality by focusing the application of the Guideline only to cloud outsourcing related to critical or important operational functions or activities. Additional comments suggested a simplification of the requirements.

EIOPA reviewed extensively the content of Guideline 8 "Risk Assessment" to ensure a better inclusion of the principle of proportionality by: (1) reducing the number of areas to check in the risk assessment; (2) focusing the scope of application of the Guideline mainly on critical or important operational functions and activities outsourced.

Due diligence

Few participants to the pubic consultation requested EIOPA to review the text of Guideline 9 "Due Diligence" making it more proportionate and risk based. Comments focused mainly on two aspects:

(1) clarify how to apply the Guideline in case an undertaking enters into a second agreement with a cloud service provider already assessed;
(2) better specify how to apply the Guideline in case of outsourcing of critical or important operational functions or activities *versus* less material outsourcing (i.e. outsourcing of non-critical or non-important operational functions or activities).

Moreover, two respondents suggested that the concept of due diligence as described by the guideline could have been confused with the concept of due diligence as described in Article 256 of Commission Delegated Regulation (EU) No 2015/35.

EIOPA reviewed extensively the text of Guideline 9 to ensure a better inclusion of the principle of proportionality. Particularly, EIOPA:

(1) included a specific paragraph in the Guideline to specify that if an undertaking enters into a second agreement with a cloud service provider already assessed by that undertaking, the undertaking should determine, on a risk-based approach, whether a second due diligence is needed;
(2) better distinguished between the due diligence to be performed on cloud service providers in case a critical or important operational function or activity is outsourced to them *versus* the due diligence on cloud service providers for less material outsourcing (i.e. outsourcing of non-critical or non-important operational functions or activities).

On the possible confusion between the term "due diligence" used in these Guidelines and the one used in Article 256 of Commission Delegated Regulation (EU) No 2015/35, EIOPA is of the opinion that there is no confusion and therefore made no changes.

Contractual requirements

The comments mainly focused on the following areas:

(1) scope of application of Guideline 10 "Contractual requirements" (i.e. outsourcing of critical or important operational functions or activities *versus* less material outsourcing[5]);
(2) relationship between Guideline 10 and the requirements set by Directive 2009/138/EC and Commission Delegated Regulation (EU) No 2015/35;
(3) changing specific contractual requirements such as: reference to cloud services pricing model, mapping of data locations, specifications of performance targets in relation to service levels, requirement for the cloud service provider to take out mandatory insurance against certain risks.

Moreover, some respondents, considering that undertakings have generally a small negotiation power against cloud providers, suggested EIOPA to liaise with cloud service providers (for example, by organising round-tables with them) to foster the

[5] i.e. outsourcing of non-critical or non-important operational functions or activities

development of a European common understanding and application of these contractual requirements.

EIOPA reviewed extensively the text of the Guideline 10 to ensure a better inclusion of the principle of proportionality. In light of this, EIOPA:

(1) reviewed the scope of application of the Guideline which will be applicable only in case of cloud outsourcing of critical or important operational functions or activities;
(2) clarified the relationship between this Guideline and the requirements set by Directive 2009/138/EC and Commission Delegated Regulation (EU) No 2015/35 by eliminating the former paragraphs 36 and 37.

Furthermore, bearing in mind the possible complexities of its implementation in case of misalignments between the content of this Guideline and of the one set by the EBA on the same subject, EIOPA further aligned the wording of this Guideline to paragraph 75 of the EBA Guidelines on outsourcing.
On the possibility to organise a workshop with cloud service providers on these Guidelines, EIOPA will evaluate this possibility in 2020.

Access and audit rights

Several comments made on Guideline 11 "Access and audit rights" mostly focused on:

(1) making the requirements of this Guideline more proportionate by focusing the application of the Guideline only to cloud outsourcing related to critical or important operational functions or activities;
(2) further increasing the possibility to rely on third-party certifications by relaxing the conditions for their use.

EIOPA clarified the scope of application of Guideline 11, which will be applicable only in case of cloud outsourcing of critical or important operational functions or activities. Furthermore, in order to foster the development of European-wide standards in the area of auditing cloud services for financial institutions, EIOPA aligned the conditions to use third-party certifications or audit reports to those set by the EBA Guidelines on outsourcing (paragraphs 92-93).
These conditions include, in case of outsourcing of critical or important operational functions or activities to cloud service providers, the requirement for the undertakings to not rely solely on third-party certifications and reports over time. This means that undertakings should not simply assume that receiving a certificate or a report is enough assurance that the cloud service is provided in accordance with their legal, regulatory and risk management obligations. If an undertaking elects to use third party certifications as audit tool, such undertaking should assess the adequacy of the information in these certifications against its own requirements and make follow-up enquiries to the cloud service providers if necessary (which might include the performance of on-site audits).

Security of data and systems

Most of the few comments on Guideline 12 "Security of data and systems" focused on (i) the removal of the requirement for the undertaking to agree on data residency policy

with the cloud service provider; (ii) the clarification of the requirements applicable in case of sub-outsourcers.

EIOPA reviewed and streamlined the content of Guideline 12 striving to further align its text to requirements set by paragraph 84 of the EBA Guidelines on outsourcing. As a result, several changes requested by the stakeholders have been included in the Guideline.

Sub-outsourcing

Few comments were made on Guideline 13 mostly focusing on making the requirements of this Guideline more proportionate and risk based.

EIOPA reviewed the entire text of Guideline 13, which has been streamlined and focused only on sub-outsourcing of critical or important operational functions or activities. These changes have been also reflected in the title of the Guideline which has been changed from "Sub-outsourcing" to "Sub-outsourcing of critical or important operational functions or activities"

Monitoring and oversight of cloud outsourcing arrangements

Few comments were made on Guideline 14 "Monitoring and oversight of cloud outsourcing arrangements" mostly focusing on making the requirements of this Guideline more proportionate and risk based.

EIOPA has reviewed the entire text of the Guideline 14, which has been streamlined by avoiding repetition of concepts/requirements included in other Guidelines. Moreover, EIOPA clarified that the main focus of monitoring should be the critical or important operational functions or activities outsourced to cloud service providers.

3. Annexes

Annex I: Guidelines on outsourcing to cloud service providers

Introduction

1. In accordance with Article 16 of Regulation (EU) No 1094/2010[6] EIOPA issues guidelines to provide guidance to insurance and reinsurance undertakings on how the outsourcing provisions set forth in Directive 2009/138/EC[7] ("Solvency II Directive") and in Commission Delegated Regulation (EU) No 2015/35[8] ("Delegated Regulation") needs to be applied in case of outsourcing to cloud service providers.
2. These Guidelines are based on Articles 13(28), 38 and 49 of the Solvency II Directive and Article 274 of the Delegated Regulation. Moreover, these Guidelines build also on the guidance provided by EIOPA Guidelines on System of Governance (EIOPA-BoS-14/253).
3. These Guidelines are addressed to competent authorities to provide guidance on how insurance and reinsurance undertakings (collectively "undertaking(s)") should apply the outsourcing requirements foreseen in the above mentioned legal acts in the context of outsourcing to cloud service providers.
4. The Guidelines apply to both individual undertakings and *mutatis mutandis* to groups[9].

   The entities subject to other sectoral requirements, which are part of a group, are excluded from the scope of these Guideline at solo level as they need to follow the sectoral specific requirements as well as the relevant guidance issued by the European Securities and Markets Authority and the European Banking Authority.
5. In case of intra-group outsourcing and sub-outsourcing to cloud service providers, these Guidelines should be applied in conjunction with the provisions of EIOPA Guidelines on System of Governance on intra-group outsourcing.
6. Undertakings and competent authorities should, when complying or supervising compliance with these Guidelines, take into account the principle of proportionality[10] and the criticality or importance of the service outsourced to cloud service providers. The proportionality principle should ensure that governance arrangements, including those related to outsourcing to cloud service providers, are proportionate to the nature, scale and complexity of the underlying risks.
7. These Guidelines should be read in conjunction with and without prejudice to EIOPA Guidelines on System of Governance and to the regulatory obligations listed in paragraph 1

[6] Regulation (EU) No 1094/2010 of the European Parliament and of the Council of 24 November 2010 establishing a European Supervisory Authority (European Insurance and Occupational Pension Authority), amending Decision No 716/2009/EC and repealing Commission Decision 2009/79/EC (OJ L 331, 15.12.2010, p. 48).

[7] Directive 2009/138/EC of the European Parliament and of the Council of 25 November 2009 on the taking-up and pursuit of the business of Insurance and Reinsurance (Solvency II), (OJ L 335, 17.12.2019, p. 1).

[8] Commission Delegated Regulation (EU) 2015/35 of 10 October 2014 supplementing Directive 2009/138/EC of the European Parliament and of the Council on the taking-up and pursuit of the business of Insurance and Reinsurance (Solvency II), (OJ L 12, 17.1.2015, p. 1).

[9] Article 212(1) of the Solvency II Directive.

[10] Article 29(3) of the Solvency II Directive.

Definitions

8. If not defined in these Guidelines, the terms have the meaning defined in the legal acts referred to in the introduction.

9. In addition, for the purposes of these Guidelines, the following definitions apply:

Service provider	means a third party entity that is performing a process, service or activity, or parts thereof, under an outsourcing arrangement.
Cloud service provider	means a service provider, as defined above, responsible for delivering cloud services under an outsourcing arrangement.
Cloud services	means services provided using cloud computing, that is, a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.
Public cloud	means cloud infrastructure available for open use by the general public.
Private cloud	means cloud infrastructure available for the exclusive use by a single undertaking.
Community cloud	means cloud infrastructure available for the exclusive use by a specific community of undertakings, e.g. several undertakings of a single group.
Hybrid cloud	means cloud infrastructure that is composed of two or more distinct cloud infrastructures.

Date of application

10. These Guidelines apply from 1 January 2021 to all cloud outsourcing arrangements entered into or amended on or after this date.

11. Undertakings should review and amend accordingly existing cloud outsourcing arrangements related to critical or important operational functions or activities with a view to ensuring compliance with these Guidelines by 31 December 2022.

12. Where the review of cloud outsourcing arrangements related to critical or important operational functions or activities is not finalised by 31 December 2022, the undertaking should inform its supervisory authority[11] of that fact, including the measures planned to complete the review or the possible exit strategy. The supervisory authority may agree with the undertaking on an extended timeline for completing that review, where appropriate.

13. The update (where needed) of the undertaking's policies and internal processes should be done by 1 January 2021 while the documentation requirements for cloud outsourcing arrangements related to critical or important operational functions or activities should be implemented by 31 December 2022.

[11] Article 13(10) of the Solvency II Directive.

Guideline 1 – Cloud services and outsourcing

14. The undertaking should establish whether an arrangement with a cloud service provider falls under the definition of outsourcing pursuant to the Solvency II Directive. Within the assessment, consideration should be given to:

a. whether the operational function or activity (or a part thereof) outsourced is performed on a recurrent or an ongoing basis; and

b. whether this operational function or activity (or a part thereof) would normally fall within the scope of operational functions or activities that would or could be performed by the undertaking in the course of its regular business activities, even if the undertaking has not performed this operational function or activity in the past.

15. Where an arrangement with a service provider covers multiple operational functions or activities, the undertaking should consider all aspects of the arrangement within its assessment.

16. In cases where the undertaking outsources operational functions or activities to service providers which are not cloud service providers but rely significantly on cloud infrastructures to deliver their services (for example, where the cloud service provider is part of a sub-outsourcing chain), the arrangement for such outsourcing falls within the scope of these Guidelines.

Guideline 2 - General principles of governance for cloud outsourcing

17. Without prejudice to Article 274(3) of the Delegated Regulation, the undertaking's administrative, management or supervisory body ("AMSB") should ensure that any decision to outsource critical or important operational functions or activities to cloud service providers is based on a thorough risk assessment, including all relevant risks implied by the arrangement such as information and communication technology ("ICT"), business continuity, legal and compliance, concentration, other operational risks, and risks associated to the data migration and/or the implementation phase, where applicable.

18. In case of outsourcing to cloud service providers of critical or important operational functions or activities, the undertaking, where appropriate, should reflect the changes in its risk profile due to its cloud outsourcing arrangements in its own risk and solvency assessment ("ORSA").

19. The use of cloud services should be consistent with the undertaking's strategies (for example, ICT strategy, information security strategy, operational risk management strategy) and internal policies and processes, which should be updated, if needed.

Guideline 3 – Update of the outsourcing written policy

20. In case of outsourcing to cloud service providers the undertaking should update the written outsourcing policy (for example, by reviewing it, adding a separate appendix or developing new dedicated policies) and the other relevant internal policies (for example, information security), taking into account cloud outsourcing specificities at least in the following areas:

a. the roles and responsibilities of the undertaking's functions involved, in particular AMSB, and the functions responsible for ICT, information security, compliance, risk management and internal audit;

b. the processes and reporting procedures required for the approval, implementation, monitoring, management and renewal, where applicable, of

cloud outsourcing arrangements related to critical or important operational functions or activities;

c. the oversight of the cloud services proportionate to the nature, scale and complexity of risks inherent in the services provided, including (i) risk assessment of cloud outsourcing arrangements and due diligence on cloud service providers, including the frequency of the risk assessment; (ii) monitoring and management controls (for example, verification of the service level agreement); (iii) security standards and controls;

d. with regard to cloud outsourcing of critical or important operational functions or activities, a reference should be made to the contractual requirements as described in Guideline 10;

e. documentation requirements and written notification to the supervisory authority regarding cloud outsourcing of critical or important operational functions or activities;

f. with regard to each cloud outsourcing arrangement that covers critical or important operational functions or activities, a requirement for a documented and, where appropriate, sufficiently tested 'exit strategy' that is proportionate to the nature, scale and complexity of the risks inherent in services provided. The exit strategy may involve a range of termination processes, including but not necessarily limited to, discontinuing, reintegrating or transferring the services included in the cloud outsourcing arrangement.

Guideline 4 - Written notification to the supervisory authority

21. The written notification requirements set in Article 49(3) of the Solvency II Directive and further detailed by EIOPA Guidelines on System of Governance are applicable to all outsourcing of critical or important operational functions and activities to cloud service providers. In case an outsourced operational function or activity previously classified as non-critical or non-important becomes critical or important, the undertaking should notify the supervisory authority.

22. The undertaking's written notification should include, taking into account the principle of proportionality, at least the following information:

a. a brief description of the operational function or activity outsourced;

b. the start date and, as applicable, the next contract renewal date, the end date and/or notice periods for the cloud service provider and for the undertaking;

c. the governing law of the cloud outsourcing agreement;

d. the name of the cloud service provider, the corporate registration number, the legal entity identifier (where available), the registered address and other relevant contact details, and the name of its parent company (if any); in case of groups, whether or not the cloud service provider is part of the group;

e. cloud services and deployment models (i.e. public/private/hybrid/community) and the specific nature of the data to be held and the locations (i.e. countries or regions) where such data will be stored;

f. a brief summary of the reasons why the outsourced operational function or activity is considered critical or important;

g. the date of the most recent assessment of the criticality or importance of the outsourced operational function or activity.

Guideline 5 – Documentation requirements

23. As part of its governance and risk management system, the undertaking should keep record of its cloud outsourcing arrangements, for example, in the form of a dedicated register kept updated over time. The undertaking should also maintain a record of terminated cloud outsourcing arrangements for an appropriate retention period subject to national regulation.

24. In case of outsourcing of critical or important operational functions or activities, the undertaking should record all of the following information:

a. the information to be notified to the supervisory authority referred to in Guideline 4;

b. in case of groups, the insurance or reinsurance undertakings and other undertakings within the scope of the prudential consolidation that make use of the cloud services;

c. the date of the most recent risk assessment and a brief summary of the main results;

d. the individual or decision-making body (for example the AMSB) in the undertaking that approved the cloud outsourcing arrangement;

e. the dates of the most recent and next scheduled audits, where applicable;

f. the names of any sub-contractors to which material parts of a critical or important operational function or activity are sub-outsourced including the countries where the sub-contractors are registered, where the service will be performed and, if applicable, the locations (i.e. countries or regions) where the data will be stored;

g. an outcome of the assessment of the cloud service provider's substitutability (for example, easy, difficult or impossible);

h. whether the outsourced critical or important operational function or activity supports business operations that are time critical;

i. the estimated annual budget costs;

j. whether the undertaking has an exit strategy in case of termination by either party or disruption of services by the cloud service provider.

25. In case of outsourcing of non-critical or non-important operational functions or activities, the undertaking should define the information to be recorded on the basis of the nature, scale and complexity of the risks inherent in the services provided by the cloud service provider.

26. The undertaking should make available to the supervisory authority, on request, all information necessary to enable the supervisory authority to perform supervision of the undertaking, including a copy of the outsourcing agreement.

Guideline 6 – Pre-outsourcing analysis

27. Before entering into any arrangement with cloud service providers, the undertaking should:

a. assess if the cloud outsourcing arrangement concerns a critical or important operational function or activity in accordance with Guideline 7;

b. identify and assess all relevant risks of the cloud outsourcing arrangement in accordance with Guideline 8;

c. undertake appropriate due diligence on the prospective cloud service provider in accordance with Guideline 9;

d. identify and assess conflicts of interest that the outsourcing may cause in line with the requirements set out in Article 274(3)(b) of the Delegated Regulation.

Guideline 7 – Assessment of critical or important operational functions and activities

28. Prior to entering into any outsourcing arrangement with cloud service providers, the undertaking should assess if the cloud outsourcing arrangement relates to an operational function or activity that is critical or important. In performing such an assessment, where relevant, the undertaking should consider whether the arrangement has the potential to become critical or important in the future. The undertaking should also reassess the criticality or importance of the operational function or activity previously outsourced to cloud service providers, if the nature, scale and complexity of the risks inherent in the agreement materially changes.

29. In the assessment, the undertaking should take into account, together with the outcome of the risk assessment, at least, the following factors:

a. the potential impact of any material disruption to the outsourced operational function or activity or failure of the cloud service provider to provide the services at the agreed service levels on the undertaking's:

   i. continuous compliance with its regulatory obligations;

   ii. short and long-term financial and solvency resilience and viability;

   iii. business continuity and operational resilience;

   iv. operational risk, including conduct, ICT and legal risks;

   v. reputational risks.

b. the potential impact of the cloud outsourcing arrangement on the ability of the undertaking to:

   i. identify, monitor and manage all relevant risks;

   ii. comply with all legal and regulatory requirements;

   iii. conduct appropriate audits regarding the operational function or activity outsourced.

c. the undertaking's (and/or group's where applicable) aggregated exposure to the same cloud service provider and the potential cumulative impact of outsourcing arrangements in the same business area;

d. the size and complexity of any undertaking's business areas affected by the cloud outsourcing arrangement;

e. the ability, if necessary or desirable, to transfer the proposed cloud outsourcing arrangement to another cloud service provider or reintegrate the services ("substitutability");

f. the protection of personal and non-personal data and the potential impact on the undertaking, policyholders or other relevant subjects of a confidentiality breach or failure to ensure data availability and integrity based on *inter alia* Regulation (EU) 2016/679[12]. The undertaking should particularly take into

[12] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), (OJ L 119, 4.5.2016, p. 1).

consideration data that is business secret and/or sensitive (for example, policyholders' health data).

Guideline 8 – Risk assessment of cloud outsourcing

30. In general, the undertaking should adopt an approach proportionate to the nature, scale and complexity of the risks inherent in the services outsourced to cloud service providers. This includes, assessing the potential impact of any cloud outsourcing, in particular, on their operational and reputational risks.

31. In case of outsourcing of critical or important operational functions or activities to cloud service providers, an undertaking should:

a. take into account the expected benefits and costs of the proposed cloud outsourcing arrangement, including weighing any significant risks which may be reduced or better managed against any significant risks which may arise as a result of the proposed cloud outsourcing arrangement.

b. assess, where applicable and appropriate, the risks, including legal, ICT, compliance and reputational risks, and the oversight limitations arising from:

   i. the selected cloud service and the proposed deployment models (i.e. public/private/hybrid/community);

   ii. the migration and/or the implementation;

   iii. the activities and related data and systems which are under consideration to be outsourced (or have been outsourced) and their sensitivity and required security measures;

   iv. the political stability and the security situation of the countries (within or outside the EU) where the outsourced services are or may be provided and where the data are or are likely to be stored. The assessment should consider:

      1. the laws in force, including laws on data protection;

      2. the law enforcement provisions in place;

      3. the insolvency law provisions that would apply in the event of a service provider's failure and any constrains that would arise with regard to the urgent recovery of the undertaking's data;

   v. sub-outsourcing, including the additional risks that may arise if the sub-contractor is located in a third country or a different country from the cloud service provider and the risk that long and complex chains of sub-outsourcing reduce the ability of the undertaking to oversee its critical or important operational functions or activities and the ability of supervisory authorities to effectively supervise them;

   vi. the undertakings overall concentration risk to the same cloud service provider, including outsourcing to a cloud service provider that is not easily substitutable or multiple outsourcing arrangements with the same cloud service provider. When assessing the concentration risk, the undertaking (and/or the Group, where applicable) should take into account all its cloud outsourcing arrangements with that cloud provider.

32. The risk assessment should be performed before entering into a cloud outsourcing. If the undertaking becomes aware of significant deficiencies and/or significant changes to the services provided or to the situation of the cloud service

provider, the risk assessment should be promptly reviewed or re-performed. In case of renewal of a cloud outsourcing arrangement concerning its content and scope (for example, enlargement of the scope or inclusion in the scope of critical or important operational functions previously not included), risk assessment should be re-performed.

Guideline 9 – Due diligence on cloud service provider

33. The undertaking should ensure in its selection and assessment process that the cloud service provider is suitable according to the criteria defined by its written outsourcing policy.

34. The due diligence on the cloud service provider should be performed prior to outsourcing any operational function or activity. In case the undertaking enters into a second agreement with a cloud service provider that has already been assessed, the undertaking should determine, on a risk-based approach, whether a second due diligence is needed. If the undertaking becomes aware of significant deficiencies and/or significant changes of the services provided or the situation of the cloud service provider, the due diligence should be promptly reviewed or re-performed.

35. In case of cloud outsourcing of critical or important operational functions, the due diligence should include an evaluation of the suitability of the cloud service provider (for example, skills, infrastructure, economic situation, corporate and regulatory status). Where appropriate, the undertaking can use to support the due diligence performed evidence, certifications based on international standards, audit reports of recognised third parties or internal audit reports.

Guideline 10 – Contractual requirements

36. The respective rights and obligations of the undertaking and of the cloud service provider should be clearly allocated and set out in a written agreement.

37. Without prejudice to the requirements defined in Article 274 of the Delegated Regulation, in case of outsourcing of critical or important operational functions or activities to a cloud service provider, the written agreement between the undertaking and the cloud service provider should set out:

a. a clear description of the outsourced function to be provided (cloud services, including the type of support services);

b. the start date and end date, where applicable, of the agreement and the notice periods for the cloud service provider and for the undertaking;

c. the court jurisdiction and the governing law of the agreement;

d. the parties' financial obligations;

e. whether the sub-outsourcing of a critical or important operational function or activity (or material parts thereof) is permitted, and, if so, the conditions to which the significant sub-outsourcing is subject to (see Guideline 13);

f. the location(s) (i.e. regions or countries) where relevant data will be stored and processed (location of data centres), and the conditions to be met, including a requirement to notify the undertaking if the service provider proposes to change the location(s);

g. provisions regarding the accessibility, availability, integrity, confidentiality, privacy and safety of relevant data, taking into account the specifications of Guideline 12;

h. the right for the undertaking to monitor the cloud service provider's performance on a regular basis;

i. the agreed service levels which should include precise quantitative and qualitative performance targets in order to allow for timely monitoring so that appropriate corrective actions can be taken without undue delay if agreed service levels are not met;

j. the reporting obligations of the cloud service provider to the undertaking, including, as appropriate, the obligations to submit reports relevant for the undertaking's security function and key functions, such as reports of the internal audit function of the cloud service provider;

k. whether the cloud service provider should take mandatory insurance against certain risks and, if applicable, the level of insurance cover requested;

l. the requirements to implement and test business contingency plans;

m. the requirement for the cloud service provider to grant the undertaking, its supervisory authorities and any other person appointed by the undertaking or the supervisory authorities, the following:

    i. full access to all relevant business premises (head offices and operation centres), including the full range of relevant devices, systems, networks, information and data used for providing the outsourced function, including related financial information, personnel and the cloud service provider's external auditors ("access rights");

    ii. unrestricted rights of inspection and auditing related to the cloud outsourcing arrangement ("audit rights"), to enable them to monitor the outsourcing arrangement and to ensure compliance with all applicable regulatory and contractual requirements;

n. provisions to ensure that the data owned by the undertaking can be promptly recovered by the undertaking in case of the insolvency, resolution or discontinuation of business operations of the cloud service provider.

Guideline 11 – Access and audit rights

38. The cloud outsourcing agreement should not limit the undertaking's effective exercise of access and audit rights as well as control options on cloud services in order to fulfil its regulatory obligations.

39. The undertaking should exercise its access and audit rights, determine the audit frequency and the areas and services to be audited on a risk-based approach, according to Section 8 of EIOPA Guidelines on System of Governance.

40. In determining the frequency and the scope of its exercise of access or audit rights, the undertaking should consider whether the cloud outsourcing is related to a critical or important operational function or activity, the nature and extent of risk and impact on the undertaking from the cloud outsourcing arrangements.

41. If the exercise of its access or audit rights, or the use of certain audit techniques creates a risk for the environment of the cloud service provider and/or another cloud service provider's client (for example, the impact on service levels, availability of data, confidentiality aspects), the undertaking and the cloud service provider should agree on alternative ways to provide a similar level of assurance and service to the undertaking (for example, the inclusion of specific controls to be tested in a specific report/certification produced by the cloud service provider).

42. Without prejudice to their final responsibility regarding the activities performed by their cloud service providers, in order to use audit resources more efficiently and decrease the organisational burden on the cloud service provider and its customers, undertakings may use:

a. third-party certifications and third-party or internal audit reports made available by the cloud service provider;

b. pooled audits (i.e. performed jointly with other clients of the same cloud service provider), or pooled audits performed by a third-party appointed by them.

43. In case of cloud outsourcing of critical or important operational functions or activities, undertakings should make use of the method referred to in paragraph 42(a) only if they:

a. ensure that the scope of the certification or the audit report covers the systems (for example, processes, applications, infrastructure, data centres, etc.) and the controls identified by the undertaking and assesses the compliance with relevant regulatory requirements;

b. thoroughly assess the content of new certifications or audit reports on an regular basis and verify that the certifications or reports are not obsolete;

c. ensure that key systems and controls are covered in future versions of the certification or audit report;

d. are satisfied with the aptitude of the certifying or auditing party (for example, with regard to rotation of the certifying or auditing company, qualifications, expertise, re-performance/verification of the evidence in the underlying audit file);

e. are satisfied that certifications are issued and that the audits are performed according to appropriate standards and include a test of the operational effectiveness of the key controls in place;

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

g. retain the contractual right to perform individual on-site audits at their discretion with regard to the cloud outsourcing of critical or important operational functions or activities; such right should be exercised in case of specific needs not possible through other types of interactions with the cloud service provider.

44. For outsourcing to cloud service providers of critical or important operational functions, the undertaking should assess whether third-party certifications and reports as referred to in paragraph 42(a) are adequate and sufficient to comply with its regulatory obligations and, on a risk based approach, should not rely solely on these reports and certificates over time.

45. Before a planned on-site visit, the party to exercise its right of access (undertaking, auditor or third-party acting on behalf of the undertaking(s)) should provide prior notice in a reasonable time period, unless an early prior notification has not been possible due to an emergency or crisis situation. Such notice should include the location and purpose of the visit and the personnel that will participate in the visit.

46. Considering that cloud solutions have a high level of technical complexity, the undertaking should verify that the staff performing the audit – being its internal

auditors or the pool of auditors acting on its behalf, or the cloud service provider's appointed auditors – or, as appropriate, the staff reviewing the third-party certification or service provider's audit reports have acquired the appropriate skills and knowledge to perform the relevant audits and/or assessments.

Guideline 12 – Security of data and systems

47. The undertaking should ensure that cloud service providers comply with European and national regulations as well as appropriate ICT security standards.

48. In case of outsourcing of critical or important operational functions or activities to cloud service providers, the undertaking should additionally define specific information security requirements in the outsourcing agreement and monitor compliance with these requirements on a regular basis.

49. For the purposes of paragraph 48, in case of outsourcing of critical or important operational functions or activities to cloud service providers, the undertaking, applying a risk based approach, and taking into account its responsibilities and the ones of the cloud service provider, should:

a. agree on clear roles and responsibilities between the cloud service provider and the undertaking in relation to the operational functions or activities affected by the cloud outsourcing, which should be clearly split;

b. define and decide on an appropriate level of protection of confidential data, continuity of activities outsourced, integrity and traceability of data and systems in the context of the intended cloud outsourcing;

c. consider specific measures, where necessary, for data in transit, data in memory and data at rest, for example, the use of encryption technologies in combination with an appropriate keys management;

d. consider the mechanisms of integration of the cloud services with the systems of the undertakings, for example, the Application Programming Interfaces and a sound user and access management process;

e. contractually ensure that network traffic availability and expected capacity meet strong continuity requirements, where applicable and feasible;

f. define and decide on proper continuity requirements ensuring adequate levels at each level of the technological chain, where applicable;

g. have a sound and well documented incident management process including the respective responsibilities, for example, by the definition of a cooperation model in case of actual or suspected incidents occur;

h. adopt a risk-based approach to data storage and data processing location(s) (i.e. country or region) and information security considerations;

i. monitor the fulfilment of the requirements relating to the effectiveness and efficiency of control mechanisms implemented by the cloud service provider that would mitigate the risks related to the provided services.

Guideline 13 – Sub-outsourcing of critical or important operational functions or activities

50. If sub-outsourcing of critical or important operational functions (or a part thereof) is permitted, the cloud outsourcing agreement between the undertaking and the cloud service provider should:

a. specify any types of activities that are excluded from potential sub-outsourcing;

b. indicate the conditions to be complied with in case of sub-outsourcing (for example, that the sub-outsourcer will also fully comply with the relevant obligations of the cloud service provider). These obligations include the audit and access rights and the security of data and systems;

c. indicate that the cloud service provider retains full accountability and oversight for the services sub-outsourced;

d. include an obligation for the cloud service provider to inform the undertaking of any planned significant changes to the sub-contractors or the sub-outsourced services that might affect the ability of the service provider to meet its obligations under the cloud outsourcing agreement. The notification period for those changes should allow the undertaking, at least, to carry out a risk assessment of the effects of the proposed changes before the actual change in the sub-outsourcers or the sub-outsourced services comes into effect;

e. ensure, in cases where a cloud service provider plans changes to a sub-outsourcer or sub-outsourced services that would have an adverse effect on the risk assessment of the agreed services, that the undertaking has the right to object to such changes and/or the right to terminate and exit the contract.

Guideline 14 – Monitoring and oversight of cloud outsourcing arrangements

51. The undertaking should monitor, on a regular basis, the performance of activities, the security measures and the adherence to agreed service level by their cloud service providers on a risk based approach. The main focus should be on the cloud outsourcing of critical and important operational functions.

52. In order to do so, the undertaking should set up monitoring and oversight mechanisms, which should take into account, where feasible and appropriate, the presence of sub-outsourcing of critical or important operational functions or a part thereof.

53. The AMSB should be periodically updated on the risks identified in the cloud outsourcing of critical or important operational functions or activities.

54. In order to ensure the adequate monitoring and oversight of their cloud outsourcing arrangements, undertakings should employ enough resources with adequate skills and knowledge to monitor the services outsourced to the cloud. The undertaking's personnel in charge of these activities should have both ICT and business knowledge as deemed necessary.

Guideline 15 – Termination rights and exit strategies

55. In case of cloud outsourcing of critical or important operational functions or activities, within the cloud outsourcing agreement the undertaking should have a clearly defined exit strategy clause ensuring that it is able to terminate the arrangement, where necessary. The termination should be made possible without detriment to the continuity and quality of its provision of services to policyholders. To achieve this, the undertaking should:

a. develop exit plans that are comprehensive, service based, documented and sufficiently tested (for example, by carrying out an analysis of the potential costs, impacts, resources and timing implications of the various potential exit options);

b. identify alternative solutions and develop appropriate and feasible transition plans to enable the undertaking to remove and transfer existing activities and data from the cloud service provider to alternative service providers or back to the undertaking. These solutions should be defined with regard to the challenges that may arise because of the location of data, taking the necessary measures to ensure business continuity during the transition phase;

c. ensure that the cloud service provider adequately supports the undertaking when transferring the outsourced data, systems or applications to another service provider or directly to the undertaking;

d. agree with the cloud service provider that once retransferred to the undertaking, its data will be completely and securely deleted by the cloud service provider in all regions.

56. When developing exit strategies, the undertaking should consider the following:

a. define objectives of the exit strategy;

b. define the trigger events (for example, key risk indicators reporting an unacceptable level of service) that could activate the exit strategy;

c. perform a business impact analysis commensurate to the activities outsourced to identify what human and other resources would be required to implement the exit plan and how much time it would take;

d. assign roles and responsibilities to manage exit plans and transition activities;

e. define success criteria of the transition.

Guideline 16 – Supervision of cloud outsourcing arrangements by supervisory authorities

57. The supervisory authorities should perform the analysis of the impacts arising from undertakings' cloud outsourcing arrangements as part of their supervisory review process. The analysis of the impacts should focus, in particular, on the arrangements related to the outsourcing of critical or important operational functions or activities.

58. Supervisory authorities should consider the following risks in the supervision of undertakings' cloud outsourcing arrangements:

a. ICT risks;

b. other operational risks (including legal and compliance risk, outsourcing and third party management risk);

c. reputational risk;

d. concentration risk, including at country/sectoral level.

59. Within their assessment, supervisory authorities should include the following aspects on a risk-based approach:

a. appropriateness and effectiveness of undertaking's governance and operational processes related to the approval, implementation, monitoring, management and renewal of cloud outsourcing arrangements;

b. whether the undertaking has sufficient resources with adequate skills and knowledge to monitor the services outsourced to the cloud;

c. whether the undertaking identifies and manages all risks highlighted by these Guidelines.

60. In case of groups, the group supervisor should ensure that the impacts of cloud outsourcing of critical or important operational functions or activities are reflected in the group supervisory risk assessment, taking into account the requirements listed in paragraphs 58-59 and the group's individual governance and operational characteristics.

61. If cloud outsourcing of critical or important operational functions or activities involves more than one undertaking in different Member states and is managed centrally by the parent company or by a group subsidiary (for example, an undertaking or a group service company such as the group ICT provider), the group supervisor and/or the relevant supervisory authorities of the undertakings involved in the cloud outsourcing, should discuss, where appropriate, the impacts of cloud outsourcing to the group risk profile in the College of Supervisors.

62. Where concerns are identified that lead to the conclusion that an undertaking no longer has robust governance arrangements in place or does not comply with regulatory requirements, supervisory authorities should take appropriate actions, which may include, for example, requiring the undertaking to improve the governance arrangement, limiting or restricting the scope of the outsourced functions or requiring to exit from one or more outsourcing arrangements. In particular, taking into account the need of ensuring continuity of the undertaking's operation, the cancellation of contracts could be required if supervision and enforcement of regulatory requirements could not be ensured by other measures.

Compliance and reporting rules

63. This document contains Guidelines issued under Article 16 of Regulation (EU) No 1094/2010. In accordance with Article 16(3) of that Regulation, competent authorities and financial institutions are required to make every effort to comply with guidelines and recommendations.

64. Competent authorities that comply or intend to comply with these Guidelines should incorporate them into their regulatory or supervisory framework in an appropriate manner.

65. Competent authorities need to confirm to EIOPA whether they comply or intend to comply with these Guidelines, with reasons for non-compliance, within two months after the issuance of the translated versions.

66. In the absence of a response by this deadline, competent authorities will be considered as non-compliant to the reporting and reported as such.

Final provision on review

67. The present Guidelines will be subject to a review by EIOPA.

Annex II: Impact assessment

Section 1 – Procedural issues and consultation of interested parties

In accordance with Article 16 of EIOPA Regulation, EIOPA conducts analyses of costs and benefits in the policy development process. The analysis of costs and benefits is undertaken according to an impact assessment methodology.

The impact assessment has been updated following the stakeholders' responses to public consultation as described in the Executive summary section.

Section 2 – Problem definition

The purchase of cloud outsourcing services falls within the broader scope of outsourcing as disciplined by the Solvency II Directive, the Delegated Regulation and clarified by the Section 11 of EIOPA Guidelines on System of Governance.

Notwithstanding the above, given the peculiarity and specificities of cloud outsourcing, there is a lack of clear and harmonized regulatory practices across European jurisdictions on the use and management of cloud outsourcing services by insurance and reinsurance undertaking. This is the core problem that the current Guidelines aim to address with the objective to provide clearer expectations on how to apply the outsourcing provisions to the use of cloud services. Taking into account that the cloud services enable undertakings to access a scalable and elastic pool of shareable physical or virtual resources with self-service provisioning and administration on-demand, a unlevel playing field (e.g. with different standards and approaches adopted by the different national supervisory authorities) could have negative impacts on the prudent cloud adoption by the European (re)insurance industry. These impacts could be summarised in: potential higher costs for the undertakings that want to outsource to cloud service providers in multiple jurisdictions and potential uncoordinated supervisory practices leading to a potential unfair competition.

EIOPA identified the above mentioned needs and decided to develop specific Guidelines on outsourcing to cloud service providers in the context of the analysis performed to answer the European Commission FinTech Action plan (COM(2018) 109 final) and following interactions with several other stakeholders[13].

The work carried out by EIOPA highlighted the following main areas that need to be clarified:

- application of the regulatory definition of outsourcing[14] to the purchase of cloud services;
- risk and materiality assessment and notification to competent authorities prior to enter into a cloud outsourcing arrangements;

[13] Please, see footnote nr.3.

[14] Article 13 (28) of Directive 2009/138/EC.

- management of specific risks associated to the use of cloud computing services (for example, data and systems security, confidentiality, legal and reputational risk, concentration risk);
- application of the audit and access requirements to cloud arrangements;
- supervision of cloud outsourcing arrangements.

Moreover, taking into account the work carried out by the European Banking Authority (EBA) in the fields of outsourcing and cloud outsourcing[15], another gap that the current draft Guidelines aim to address is the lack of guidance for the regulatory framework and supervisory assessment of outsourcing risks in EU insurance and reinsurance undertakings and therefore room for inconsistency in assessing outsourcing risk across jurisdictions[16] leading to a lack of comparability of supervisory practices across EU which is of crucial importance given the cross-border nature of the cloud service. Inconsistency in the treatment of potential risks related to cloud services may also lead to an unlevel playing field across jurisdictions and undertakings.

When analyzing the impact from proposed policies, the impact assessment methodology foresees that a baseline scenario is applied as the basis for comparing policy options. This helps to identify the incremental impact of each policy option considered. The aim of the baseline scenario is to explain how the current situation would evolve without additional regulatory intervention.

For the analysis of the potential related costs and benefits of these Guidelines, EIOPA has applied as a baseline scenario the effect from the application of the current general requirements on outsourcing in the Solvency II framework. In particular the baseline includes:

- Article 49 of the Solvency II Directive;
- Article 274 of the Delegated Regulation;
- Section 11 of EIOPA Guidelines on system of governance.

Section 3 – Objectives pursued

The main objective of these Guidelines is to specify a set of principle-based rules in order to provide clarity on how the outsourcing provisions shall be applied by insurance and reinsurance undertakings to the purchase of cloud services.

Moreover, the principle-based rules provide the supervisory authorities with a common regulatory framework and tools that should be considered as minimum European standard, in their risk assessment of risks arising from cloud outsourcing. This is further

[15] Namely the EBA Guidelines on outsourcing arrangements (EBA/GL/2019/02) and the EBA Recommendations on outsourcing to cloud service providers (EBA/REC/2017/03), which have been integrated into the EBA Guidelines on outsourcing and are repealed with effect from 30 September 2019.

[16] On the basis of the analysis performed by EIOPA in 2018 as part of the answer the European Commission FinTech Action plan, the current level of national guidance on cloud outsourcing for (re)insurance sector is not homogenous. For example as at 31 December 2018:

- In CZ, DE, FI, FR, PL, SE, UK-FCA, national guidance on cloud outsourcing applicable to the financial sector including (re)insurance have been published by the NSA.
- In ES, IT, LV, RO, FR, NL, there are broader national standards to support the management of specific critical areas of cloud outsourcing.
- In GR, PT and IE there is not a specific plan.

expected to lead to the harmonisation of the practices and a common level-playing field across jurisdictions.

The mentioned objectives for the Guidelines are connected to the general objectives of the Solvency II framework (deepen the integration of the EU insurance market, enhance the protection of policyholders and beneficiaries and promote better regulation) and in particular they are connected to:

- the improvement of governance and risk management for insurance and reinsurance undertakings;
- the harmonisation of supervisory methods; and
- the promotion of compatibility of prudential supervision of insurance and banking.

The objectives of the Guidelines are also consistent with the following objectives of EIOPA, as reflected in the Regulation of the Authority:

- ensure a sound, effective and consistent level of regulation and supervision;
- ensure the taking of risks related to (re)insurance activities is appropriately regulated and supervised; and
- consumer protection.

Section 4 – Policy options

With the aim to meet the objectives set out in the previous section, EIOPA has analysed different policy options throughout the policy development process.

The section below reflects the most relevant policy options that have been considered in relation to the different aspects associated to the cloud outsourcing process. We have also listed relevant options which have been discarded in the policy development process.

Policy issue 1: Introduction of the Guidelines versus the status quo

Policy option 1.1 Introduction of EIOPA cloud outsourcing Guidelines to provide clarity on how the outsourcing provisions shall be applied by insurance and reinsurance undertakings to the purchase of cloud services.

Policy option 1.2 Keeping the status quo not issuing any guidance on the subject.

Policy issue 2: Development of dedicated cloud outsourcing Guidelines versus development of more detailed Guidelines on outsourcing arrangements as a whole

Policy option 2.1 Development of dedicated EIOPA cloud outsourcing Guidelines built on the current outsourcing provisions and the EBA work in the field of outsourcing.

Policy option 2.2 Development of more detailed and specific Guidelines on outsourcing arrangements which include also the specificities of Guidelines on outsourcing to cloud service providers. The Guidelines on outsourcing arrangement would build on the EBA work in the field of outsourcing.

Policy issue 3: The purchase of cloud services falls always under the scope of outsourcing versus assessment on the basis of the function outsourced

Policy option 3.1 Insurance and reinsurance undertakings should consider all the purchase of cloud services as outsourcing and then apply to all of them the regulatory requirements and these Guidelines.

Policy option 3.2: Insurance and reinsurance undertakings in case of purchase of cloud services, should perform an assessment to understand whether these services fall within the scope of outsourcing. Only on these ones, the regulatory requirements and these Guidelines shall apply. As a rule and starting point, outsourcing is assumed.

Policy option 3.3: Insurance and reinsurance undertakings in case of purchase of cloud services should perform an assessment to understand whether these services fall within the scope of outsourcing. Only on these ones, the regulatory requirements and these Guidelines shall apply. This option has been identified based on the feedback to the public consultation.

Policy issue 4: Documentation requirements

Policy option 4.1 Requiring insurance and reinsurance undertakings to document all their cloud outsourcing arrangements providing a detailed list of information to be kept (i.e. in the form of a register).

Policy option 4.2: Keep the status quo (i.e. the undertakings are free to define their own way of documenting their cloud arrangements in place).

Policy option 4.3: Definition of the elements to be recorded by insurance and reinsurance undertakings in case of cloud outsourcing of critical or important operational functions and activities and keeping the status quo in case of outsourcing to cloud service providers of non-critical non-important operational functions and activities. This option has been identified based on the feedback to the public consultation.

Policy issue 5: Role for college of supervisors in the written notification process before outsourcing to cloud service providers critical or important operational functions or activities *versus* the status quo

Considering the nature of cloud services, sometimes insurance and reinsurance groups manage centrally through the parent company or another subsidiary (such as an undertaking or a group service company, e.g. the group ICT provider) the design, the deployment and the monitoring of cloud services that involve more than one undertaking belonging to the group. In these cases, usually the following activities are performed centrally (short list):

- definition of business requirements,;
- materiality and risk assessment of the services outsourced and of the provider(s);
- managing and coordinating the implementation/migration activities;
- building of the service monitoring team;
- managing of the relationship with the service provider from a legal (e.g. contractual) and operational perspective.

In light of the above, in case of cross-border groups, in the context of cloud outsourcing of critical or important operational functions or activity that involve more than one undertaking belonging to the same group and that is managed centrally by the parent company or by a group subsidiary (for example, an undertaking or a group service company such as the group ICT provider):

Policy option 5.1: giving the possibility, under certain circumstances, to insurance and reinsurance undertakings to submit the written notification required by Article 49 (3) Directive 2009/138/EC in the context of the College of Supervisors (i.e. one notification per group for the undertakings included in the scope of proposed cloud outsourcing).

Policy option 5.2: Requiring insurance and reinsurance undertakings to submit the written notification required by Article 49 (3) Directive 2009/138/EC keeping the status quo (i.e. one notification per undertaking) and recommending the supervisory authorities to make use of the College of Supervisors to supervise, in a preventive way, the impact of such type of outsourcing to the group's risk profile.

Section 5 – Analysis of impacts

Policy issue 1: Introduction of the Guidelines versus the status quo

Policy option 1.1 Introduction of EIOPA cloud outsourcing Guidelines to provide clarity on how the outsourcing provisions shall be applied by insurance and reinsurance undertakings to the purchase of cloud services.

On the basis of the analysis performed by EIOPA to answer the European Commission FinTech Action plan, taking into account the work already performed by the EBA and the fact that some jurisdictions have issued or planned to issue guidance on cloud outsourcing, EIOPA has identified the lack of legal transparency and potential regulatory arbitrages as risks for the market participants (i.e. regulated undertakings and service providers). Moreover, EIOPA has identified several specific risks associated to cloud outsourcing that these Guidelines aim at mitigating.

Particularly, EIOPA is the opinion that the introduction of new Guidelines on outsourcing to cloud service providers aligned to the work already performed by EBA:

a) supports the (re)insurance undertakings in their prudent transition to the cloud, providing clarity on the application of regulatory requirements, and, therefore, unlocking the opportunities that this technology provides;

b) provides a framework for cloud outsourcing for (re)insurance undertakings aligned to the one set for banking and payment institutions, enabling the scalability of the investments already made by service providers to achieve their compliance. Moreover, it gives them the possibility to provide additional services (e.g. cloud service provider compliance programs) to the industry at a fraction of the cost;

c) maximise the investments made in terms of supervisory skills and knowledge by the national supervisory authorities who supervise – in addition to the (re)insurance– the banking or the payment markets;

d) increases the protection of the policyholders in case their insurance providers uses cloud services.

In terms of cost of compliance with the Guidelines, it is reasonable to expect that the jurisdictions where the current practices overlap or show similarities with what is proposed in these draft Guidelines will bear less administrative cost both for the undertakings and the competent authorities. This is expected particularly for those jurisdictions where the insurance competent authorities are the same as those for the banking sector. In other words, the more similar are the current practices to the Guidelines the less costly will be transition is going to be. Furthermore, potential additional costs for the industry could be expected due to the chargebacks by cloud service providers to the undertakings due to the introduction of specific contracts clauses.

Policy option 1.2 Keeping the status quo not issuing any guidance on the subject.

EIOPA believes that, without the introduction of the additional guidance, the current set of Guidelines on outsourcing fail to provide an adequate regulatory framework for the insurance and reinsurance undertakings and the competent authorities in their handling of cloud outsourcing activities in the insurance and reinsurance sector.

Moreover, without the issuance of guidance on the subject the entire industry faces the risk to develop non-homogenous practices to apply the outsourcing requirements to the purchase of cloud services.

Finally, without the issuance of guidance there is the risk that negotiating non-standard contractual clauses (i.e. financial services and insurance specific clauses) with cloud service providers would be challenging in particular for smaller undertakings. This could cause higher operational risks for the entire industry with potential impacts on the policyholders (e.g. in case of wrong data or location management).

Policy issue 2: Development of dedicated cloud outsourcing Guidelines versus development of more detailed Guidelines on outsourcing arrangements as a whole

As reported above, while performing its assessment on the development of these Guidelines, EIOPA has taken into account the work carried out by the EBA in the fields of outsourcing and cloud outsourcing. Particularly, the EBA issued in 2017 their Recommendations on cloud outsourcing (EBA/REC/2017/03) and in 2019 the EBA Guidelines on outsourcing arrangements (EBA/GL/2019/02) which have repealed the Recommendations absorbing their text.

On the basis of the results of the internal assessment mentioned in the previous paragraph, EIOPA believes that the risks arising from the usage of cloud computing by (re)insurance undertakings are, generally, aligned to the risks bear by the banking players with few minor (re)insurance specificities.

The analysis of impacts on the Policy issue nr.2 takes into account the above.

Policy option 2.1 Development of dedicated EIOPA cloud outsourcing Guidelines build on the current outsourcing provisions and the EBA work in the field of outsourcing.

Notwithstanding the fact that the purchase of cloud computing services falls within the broader scope of outsourcing, the use of cloud services has some conceptual differences from the traditional ICT outsourcing. One above all is that the cloud customer does not receive from the cloud provider dedicated ICT resources (such as: servers, storage or networking) as it happens in traditional ICT outsourcing configurations.

The issuance of specific guidance on cloud outsourcing gives the possibility to provide clarity and homogeneity across member states on how to apply the framework on outsourcing to cloud computing while minimising the impacts on the insurance and insurance undertakings.

In order to avoid inconsistencies between the banking and the insurance sector, the Guidelines build on the:

- EBA Recommendations on cloud outsourcing (EBA/REC/2017/03) and;
- EBA Guidelines on outsourcing arrangements (EBA/GL/2019/02).

Policy option 2.2 Development of more detailed and specific Guidelines on outsourcing arrangements which include also the specificities of Guidelines on outsourcing to cloud service providers. The Guidelines on outsourcing arrangement would build on the EBA work in the field of outsourcing.

The issuance of new more detailed and specific Guidelines on outsourcing arrangements which include has the main benefits of: (i) keeping a consistent approach to the banking sector and (ii) minimising therefore the risk of having an additional limited implementation effort for the jurisdictions that have applied the EBA Guidelines on outsourcing also to the insurance sector.

However, the issuance of more detailed Guidelines on outsourcing arrangements built on the EBA ones, poses the risk of potential more significant implementation costs for the insurance undertakings.

Moreover, considering the market trends of expected broader and more intense use of cloud services by insurance and reinsurance undertakings, the issuance of specific guidance to ensure greater harmonization of the regulatory practices across the market on outsourcing to cloud service providers has been considered as a priority by EIOPA.

Policy issue 3: The purchase of cloud services falls always under the scope of outsourcing versus assessment on the basis of the function outsourced

Policy option 3.1 Insurance and reinsurance undertakings should consider all the purchase of cloud services as outsourcing and then apply to all of them the regulatory requirements and these Guidelines.

Considering the use of cloud services as always outsourcing provides a clear and simple framework to be applied to the purchase of cloud services and it would simplify the understanding the scope of cloud outsourcing.

However, this approach would cause additional costs to both the regulated undertakings and the service providers. Moreover, the approach under the policy option 3.1 would

not be fully in line with the current market practices associated to outsourcing arrangements causing potential additional investments and running costs for the undertakings to comply with it.

In other words, although the approach under the policy option 3.1 appears to be sound to capture and manage the risks posed to the undertakings in case they decide to use cloud services, it appears to be not fully proportionate.

Policy option 3.2: Insurance and reinsurance undertakings in case of purchase of cloud services, should perform an assessment to understand whether these services fall within the scope of outsourcing. Only on these ones, the regulatory requirements and these Guidelines shall apply. As a rule and starting point, outsourcing is assumed.

Letting the undertakings to perform their own assessments to classify their purchase of cloud services as outsourcing would pose risks of lack of homogeneity among the application of the provisions across jurisdictions.

However, if complemented with clear principle-based instructions and under the presumption that outsourcing in a regulated context should be assumed, the approach under the policy option 3.2 appears to be both proportionate and sound to capture and manage the risks posed to the undertakings in case they decide to use cloud services.

Moreover, being the approach under the policy option 3.2 closer to the current practice, choosing it would result in lower costs of compliance for the regulated undertakings and the service providers.

Policy option 3.3: Insurance and reinsurance undertakings in case of purchase of cloud services, should perform an assessment to understand whether these services fall within the scope of outsourcing. Only on these ones, the regulatory requirements and these Guidelines shall apply.

The approach foreseen by Policy option 3.3 is the same as the policy approach 3.2 with the only difference that under Policy 3.3 the presumption that all arrangements with cloud service providers are to be considered as outsourcing has been removed.

The approach 3.3 has been developed thanks to the feedback to the public consultation. As reported in the feedback statement, in order to align the Guideline to the current practices in place for outsourcing, to make them more proportionate and in line to the approach chosen by the EBA in their outsourcing Guideline, the presumption described above was removed.

Policy issue 4: Documentation requirements

Policy option 4.1 Requiring insurance and reinsurance undertakings to document their cloud outsourcing arrangements providing a detailed list of information to be kept (i.e. in the form of a register).

The policy option 4.1 could generate higher upfront costs for the undertakings which do not have structured approaches to manage their cloud outsourcing arrangements. However, due to the simplicity to access to the cloud and set up contractual

arrangements with the cloud service providers, requiring the undertakings to document their outsourcing arrangements and keep them in a structured central register could support them in the application of sound risk management approach in the decision to outsource to cloud service providers and in the management of such services including the related concentration risks.

Furthermore, the policy option 4.1 being aligned to the approach adopted by the EBA reduces the risk of unneeded cross-sectoral differences.

Policy option 4.2: Keep the status quo (i.e. the undertakings are free to define their own way of documenting their cloud arrangements in place).

The policy option 4.2 produces lower upfront costs to set up the documentation process for the undertakings which do not have structured approaches to manage their cloud outsourcing arrangements. However, in the long run, the policy option 4.2 could produce a risk of non-homogeneity of interpretation of the requirements set by these Guidelines and the risk of unmanaged operational risks which could result in higher costs for the undertakings at a later stage.

Policy option 4.3: Definition of the elements to be recorded by insurance and reinsurance undertakings in case of cloud outsourcing of critical or important operational functions and activities and keeping the status quo in case of outsourcing to cloud service providers of non-critical non-important operational functions and activities.

EIOPA developed the policy option 4.3 as response to the feedback to the public consultation as described in the Feedback Statement.

This approach requires the undertaking to keep record of all their outsourcing arrangements without specifying the format of their recording. Furthermore, the approach under policy option 4.3 specifies a minimum set of information to be kept recorded only for outsourcing arrangements related to critical or important operational functions or activities.

Policy issue 5: Role for college of supervisors in the written notification process before outsourcing to cloud service providers critical or important operational functions or activities *versus* the status quo

Policy option 5.1: giving the possibility, under certain circumstances, to insurance and reinsurance undertakings to submit the written notification required by Article 49 (3) Directive 2009/138/EC in the context of the College of Supervisors (i.e. one notification per group).

In case of cross-border groups, in the context of cloud outsourcing of critical or important operational functions or activities that involve more than one undertaking belonging to the same group and that is managed centrally by the parent company or by a group subsidiary (e.g. an undertaking or a group service company such as the group ICT provider), the policy option 5.1 gives the possibility, as an option, to perform the written notification process at the level of College of Supervisors could provide several benefits to:

- the insurance and reinsurance groups in terms, for instance, of reduced administrative burdens by performing one notification instead of several;
- the regulatory community that can have a more transparent dialogue with the experts of the group on the field of cloud computing with the possibility to share their supervisory concerns at the highest hierarchical level of the group increasing, therefore, the efficiency and effectiveness of their preventive supervision.

Furthermore, the approach described under the policy option 5.1 could increase the consistency in the supervisory practices on the subject of cloud outsourcing and ICT risk management of the undertakings belonging to the group and of the group as a whole.

However, the operational feasibility of policy option 5.1 appears to be limited, particularly considering the fact that:

(i) the notification requirements for outsourcing of critical or important operational functions or activities have been adopted in a non-homogeneous way by Member States, and

(ii) in any case, the adoption of the policy option 5.1 will not grant any exemption to the group to follow the national laws and regulations that may apply to the cloud outsourcing arrangement which would be notified to the College of Supervisors.

Policy option 5.2: requiring insurance and reinsurance undertakings to submit the written notification required by Article 49 (3) Directive 2009/138/EC keeping the status quo and recommending the supervisory authorities to make use of the College of Supervisors to supervise, in a preventive way, the impact of such type of outsourcing to the group's risk profile.

Taking into account the characteristics of cloud services and the activities performed in case of group-led cloud outsourcing initiatives (reported at the paragraph describing the policy option 5.1), and considering that a sound an prudent use of cloud computing is an enabler for innovation in the financial sector, keeping the status quo could have a negative impact on the adoption of the cloud for the undertakings – member of cross-border groups – established in the jurisdictions that do not constitute the first operational priority for the groups.

However, taking into account the operational limitations presented at the paragraph describing the policy option 5.1, there are risks of increasing the complexity of the cloud computing notification process, affecting therefore the time-to-market of the re(insurance) undertakings electing to use this possibility.

Furthermore, the policy option 5.2, incorporating a specific recommendation to the supervisory community to make use of the College of Supervisors to effectively supervise the group outsourcing of critical or important operational functions or activities to cloud service providers, appear to foster the increase of transparency and communication among the relevant supervisory authorities.

Section 6 – Comparison of options

Regarding policy options 1.1 and 1.2 on the basis of the previous section and taking into account the future trends of increasing usage of cloud services by European (re)insurers, **EIOPA has chosen the policy option 1.1** "Introduction of EIOPA cloud outsourcing Guidelines to provide clarity on how the outsourcing provisions shall be applied by insurance and reinsurance undertakings to the purchase of cloud services". EIOPA believes that the introduction of these Guidelines could support the European insurance market risk based outsourcing to cloud service providers.

Regarding policy options 2.1 and 2.2 on the basis of the previous section and considering the preparatory analysis performed in the context of developing its answer to the European Commission FinTech Action Plan[17], **EIOPA has chosen the policy option 2.1** "Development of dedicated EIOPA cloud outsourcing Guidelines built on the current outsourcing provisions and the EBA work in the field of outsourcing" in order to, timely, answer the increasing market practices of outsourcing to cloud service providers by providing Guidelines. However, taking into account the feedback to the Public consultation, in the process of reviewing the System of Governance Guidelines, EIOPA will evaluate the option to merge these Guidelines with the updated version of the Guideline on outsourcing.

Regarding policy options 3.1, 3.2 and 3.3, on the basis of the previous section and of the feedback to the public consultation with the aim of creating the minimum disruption as possible to the current practices observed in the market while, at the same time, ensuring a sound risk management of the purchase of cloud services, **EIOPA has chosen the policy option 3.3** "Insurance and reinsurance undertakings in case of purchase of cloud services, should perform an assessment to understand whether these services fall within the scope of outsourcing. Only on these ones, the regulatory requirements and these Guidelines shall apply."

Taking into account the feedback to the public consultation, **EIOPA has chosen the policy option 4.3** "Definition of the elements to be recorded by insurance and reinsurance undertakings in case of cloud outsourcing of critical or important operational functions and activities and keeping the status quo in case of outsourcing to cloud service providers of non-critical non-important operational functions and activities." As reported in the Feedback section above, EIOPA acknowledges that the changes made are a major departure from the requirements set by the EBA Guidelines on outsourcing, which requires firms to maintain a register on all outsourcing arrangements. This decision was taken under the assumption that a broader and comprehensive discussion on how document the outsourcing arrangements will be undertaken when reviewing the System of Governance Guidelines. In any case, when evaluating the compliance to that requirement, the supervisory authorities should take particularly into account the principle of proportionality as defined by Article 29 of Solvency II Directive.

Regarding policy options 5.1 and 5.2 on the basis of the previous section and considering the potential legal and operational limitations of the policy option 5.1, , **EIOPA has chosen the policy option 5.2** "Requiring insurance and reinsurance

[17] Please, see footnote nr.2.

undertakings to submit the written notification required by Article 49(3) Directive 2009/138/EC keeping the status quo and recommending the supervisory authorities to make use of the College of Supervisors to supervise, in a preventive way, the impact of such type of outsourcing to the group's risk profile"

Annex III: Resolution of comments

Insurance associations

Insurance Europe, Belgium

Response to the public consultation question	EIOPA's comments
1. 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, i.e. 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 (i.e. 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	**EIOPA partially agrees with the concerns raised by the respondent.** In case of outsourcing, an undertaking has to ensure that it remains fully responsible for discharging all its obligations when outsourcing any function or activities (as stated in EIOPA system of governance paragraph 1.14). For the outsourcing of critical or important operational functions or activities, an undertaking must meet a number of requirements. In light of this, aiming at embedding the principle of proportionality and a risk-based approach, EIOPA streamlined the contents of the Guidelines, which are simpler and mainly focusing on outsourcing of critical or important operational functions or activities to cloud service providers. However, some of the provisions are applicable also to outsourcing of non-critical, non-important operational functions or activities. On the Guidelines cited by the respondent: - in Guideline 3, in addition to other changes, EIOPA clarified that the application of paragraph 20(former 16) point (d) and (f) is expected in case of outsourcing to cloud service providers of critical or important operational functions or activities; - EIOPA significantly streamlined the content of Guideline 5 (i.e. no specific requirements for keeping a register but to record information). Moreover, EIOPA has defined, as minimum requirement, a set information to be recorded only for critical or important operational functions outsourced to cloud service providers; - in Guideline 11, EIOPA clarified that the Guideline is applicable only in case of cloud outsourcing of critical or important operational functions or activities. On the basis of the feedback received and bearing in mind that one of the main purposes of these Guidelines is to provide clarity to the market participants, EIOPA decided to withdraw the use of the term "material outsourcing" sticking to the term "critical or important operational function and activity". Finally, on the respondent request to include criteria for cloud services falling outside the scope of outsourcing, considering that some examples have

Response to the public consultation question	EIOPA's comments
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.	already been included in the explanatory text of the EIOPA Guidelines on system of governance, EIOPA has decided to not include in the Guidelines examples of cloud services that are not to be considered as outsourcing. **EIOPA updated the Guidelines accordingly**
2. 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	**EIOPA partially agrees with the concerns raised by the respondent.** On the definition of Material outsourcing, on the basis of the feedback received and bearing in mind that one of the main purposes of these Guidelines is to provide clarity to the market participants, EIOPA decided to withdraw the use of the term "material outsourcing" sticking to the term "critical or important operational function and activity". The definition has been deleted Public cloud, in order to have market consistency the definition has been kept aligned to the one used in the EBA Guidelines on outsourcing. No changes have been made. Private cloud, in order to have market consistency the definition has been kept aligned to the one used in the EBA Guidelines on outsourcing. No changes have been made. Function, in order to avoid the possible confusion with Article 13(29) of Solvency II Directive, EIOPA decided to delete the definition. The definition has been deleted. Cloud service provider, the definition has been clarified. Cloud broker, as the concept of cloud broker is not used in the Guidelines, EIOPA decided to delete the definition. The definition has been deleted. Non-material outsourcing, EIOPA decided not to include the definition as the definition of "Material outsourcing" has been deleted. No changes made

Response to the public consultation question	EIOPA's comments
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 (i.e. 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, e.g. 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." 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 (e.g. 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.	

Response to the public consultation question	EIOPA's comments
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.	
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?	
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 (e.g. 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	**EIOPA partially agrees with the concerns raised by the respondent.** EIOPA moved the date of application to 1 January 2021 and prolonged the period for transitional arrangements to 31 December 2022. Furthermore, clarification on the due date to perform the update (where needed) the undertaking policies and internal processes in accordance to the Guidelines has been clarified and set to 1 January 2021. On the proposal to grandfather the existing obligation, EIOPA has not agreed with the proposal. However, in order to make the Guidelines more proportionate, a principle of risk-based review has been introduced (i.e. only contract related to critical and important operational functions should be amended). Furthermore, the flexibility clause contained in the draft version of the Guidelines (paragraph 9) has been kept. **EIOPA updated the Guidelines accordingly.**

Response to the public consultation question	EIOPA's comments
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 (i.e. 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.	
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?	
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, e.g. 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 (e.g. 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	**EIOPA partially agrees with the concerns raised by the respondent.** The determination of whether (or not) the purchase of cloud services fall into the scope of outsourcing is paramount to a successful and coherent application of these Guidelines. To perform this determination is responsibility of the undertakings and should be carried out by applying the criteria provided in Guideline 1 and in the regulatory obligations listed in the introduction of these Guidelines. There are two type of arrangements with third parties: 1) Services which are not outsourcing (for example, non-recurrent activities – as detailed in Guideline 1 – and purchases of goods – including software licences – are not considered as outsourcing arrangements) and 2) Services, which are outsourcing. Among the services which are outsourcing there is a distinction between: - outsourcing of critical or important operational functions (which includes, but is not limited to, insurance and reinsurance processes and activities, functions as defined by Solvency II art. 13(29), provisioning of on-going day to day

Response to the public consultation question	EIOPA's comments
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 (i.e. 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	systems maintenance or support, investment of assets or portfolio management, etc.) - outsourcing of non-critical, non-important operational functions (i.e. less material). In case of any outsourcing (regardless if it of critical or important operational functions) an undertaking has to ensure that it remains fully responsible for discharging all its obligations when outsourcing any function or activities (as stated in EIOPA System of Governance paragraph 1.14). For the outsourcing of critical or important operational functions or activities, an undertaking must meet certain requirements. When an undertaking purchases cloud services, it should perform the same type of assessment due in case of "general outsourcing", namely 1) understand whether the purchase of cloud services is outsourcing or not; 2) if it classifies as outsourcing, understand whether the outsourced function is critical or important; 3) on critical or important operational functions or activities, perform a detailed risk assessment on the operational function/activity to be outsourced and a detailed due diligence on the service provider; 4) On all the less material outsourcing, in order to fulfil its responsibility obligation (as stated above), a risk assessment and a due diligence (of higher level compared to the previous point) are to be performed. Furthermore, notwithstanding the results of the assessment of whether the provisioning of cloud services falls under the definition of "outsourcing", as part of their internal control system, on a risk and proportionate way, the undertaking should identify, measure, monitor, manage and report risks caused by arrangements with third parties regardless whether or not those third parties are cloud service providers. On the respondent request to eliminate the sentence "as a rule outsourcing should be assumed" from the Guideline, in light of the above, EIOPA deleted that sentence. On the respondent request to eliminate the former paragraph 12 of the draft Guidelines, recognising that the focus of the Guidelines is cloud outsourcing, EIOPA deleted that paragraph. On the respondent request to include examples if cloud services falling outside the scope of outsourcing, considering that some examples have already been included in the explanatory text of the EIOPA Guidelines on system of

Response to the public consultation question	EIOPA's comments
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 (i.e. "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 whether this function (or a 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.	governance, EIOPA has decided to not include in the Guidelines examples of cloud services that are not to be considered as outsourcing. On the request to change the criteria provided by Guideline 1, EIOPA simplified those criteria bearing in mind the policy objective to align them to the ones included by the EBA in their Guidelines on outsourcing. **EIOPA updated the Guidelines accordingly.**
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?	
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.	**EIOPA partially agrees with the concerns raised by the respondent.** EIOPA has decided to keep the Guideline 3 clarifying its application. For this reason, as the Solvency II principles on outsourcing are still valid for cloud, with reference to the update of internal policies and procedures, multiple solutions are at disposal for undertakings: 1) development – where needed – of a dedicated cloud outsourcing policy; 2) complement - where needed – the undertaking outsourcing policy and the other relevant internal policies (for example, the information security policy) to take into account the specificities of outsourcing to cloud service providers; and 3) if the undertaking current policies cover the elements described in these Guidelines, there is no need to update. EIOPA has also enhanced the focus of the requirements toward the outsourcing of critical or important functions or activities to cloud service providers.

Response to the public consultation question	EIOPA's comments
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, i.e. 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.	On the point raised concerning Guideline 2 (i.e. role of the AMSB), EIOPA agrees with the concerns raised by the respondent and clarified the role of the AMSB in line to the mentioned regulatory requirement. **EIOPA updated the Guidelines accordingly.**
5b. Is the Guideline on written policy consistent to the market best practices on defining the policy for general outsourcing?	
See answer above	NA
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?	
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	**EIOPA partially agrees with the concerns raised by the respondent.** The content of Guideline 4 which is related only to outsourcing of critical or important operational functions or activities has been streamlined by: (a) removing the requirement to present a draft copy of the outsourcing

Response to the public consultation question	EIOPA's comments
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 (i.e. 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.	agreement (b) aligning the requirements to the EBA requirements set by paragraph 54 of the EBA Guidelines on outsourcing to ensure market consistency for outsourcing to cloud service providers. On the point related to former paragraph 18(f), EIOPA agrees with the concern that service models are constantly evolving and has removed the references to SaaS, IaaS and PaaS (and the related definitions) and replaced this text with a more generic reference to 'cloud service models'. With reference to the clarifications requested by the respondent: - On the outcome of the notification, being the requirements for outsourcing valid and applicable also in the context of cloud outsourcing, EIOPA is the opinion that the notification shall be used by National Authorities according to the current rules practices related Outsourcing (i.e. if the notification is for information will continue to be for information and if it is for approval, it will continue be for approval). However, among other things, in order to foster supervisory convergence in the practice of written notification, during the review of the system of governance Guidelines the option of introducing a clearer and more convergent approach on Notifications and Documentation requirements will be further analysed. - On the timing when the undertakings are expected to notify their national supervisory authorities, EIOPA agrees with the respondent (i.e. the notification is to be performed before outsourcing); - On the submission of the outsourcing arrangement as part of the written notification, although requiring the undertakings to submit the outsourcing arrangement as part of the written notification is a practice already in place in some European countries, as reported above, EIOPA deleted the requirement; - On the "change of status" of a cloud outsourcing arrangement, EIOPA clarified that the undertakings should re-submit the notification only if the outsourced operational functions or activities previously classified as non-critical non-important become critical or important. **EIOPA updated the Guidelines accordingly.**

Response to the public consultation question	EIOPA's comments
- 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.	
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?	
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, e.g. 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	**EIOPA partially agrees with the concerns raised by the respondent.** EIOPA has streamlined the content of the Guideline 5 in order to make it more principle and risk based by removing the requirements for keeping a register and requiring the undertaking to record information of their cloud outsourcing arrangements. Furthermore, EIOPA has defined, as minimum requirement, a set information to be recorded only for critical or important operational functions outsourced to cloud service providers. This set of information is aligned to the one required by the EBA Guidelines on Outsourcing. For outsourcing to cloud service providers on non-critical non-important operational functions or activities, the level of detail of the information to be recorded should be determined by the undertakings on a risk-based approach. The requirement to keep information on ended outsourcing arrangements is the same as the included in the EBA Guidelines on Outsourcing (paragraph 52). As requested by the respondent EIOPA clarified that an undertaking should define the appropriate retention period taking into account national regulation and the principle of proportionality. **EIOPA updated the Guidelines accordingly.**

Response to the public consultation question	EIOPA's comments
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 (i.e. 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 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 (e.g. data centre provider).	

Response to the public consultation question	EIOPA's comments
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.	
7b. What can be other approaches to ensure a proper and sound holistic oversight of cloud outsourcing?	
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.	**EIOPA noted the concerns raised by the respondent.** EIOPA will take the suggestion into account in the process of reviewing the System of Governance Guidelines when a broader and comprehensive discussion on how document the outsourcing arrangements will be undertaken. **No changes were made to the Guidelines.**
8. 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 (e.g. paragraph 27(e) etc.).	**EIOPA partially agrees with the concerns raised by the respondent.** In particular, EIOPA: - clarified that records should be kept for cloud outsourcing arrangements related to critical or important operational functions or activities. - being the information on budget costs a possible metric of the significance of the provider, kept the requirement to record it. Moreover, in order to clarify the purpose, EIOPA aligned the wording to the one used by the EBA in its Guidelines on outsourcing; - removed the requirement to record a description of the undertaking monitoring of the cloud outsourcing activities.

Response to the public consultation question	EIOPA's comments
We also suggest the removal of paragraph 23(i) (i.e. 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 (e.g. ISO 27001).	In order to minimise the risk of possible different local applications to the requirements of paragraphs 21 to 26 (former 18 to 23), when applicable, EIOPA aligned the wording of the Guidelines to the EBA Guidelines on outsourcing. **EIOPA updated the Guidelines accordingly.**
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?	
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	**EIOPA partially agrees with the concerns raised by the respondent.** On the use of the term "material" instead of the term "critical or important", as reported above, bearing in mind that one of the main purposes of these Guidelines is to provide clarity to the market participants, EIOPA decided to withdraw the use of the term "material outsourcing" sticking to the term "critical or important operational function and activity". On the other specific comments, EIOPA: - clarified the paragraph 27(c) (former paragraph 24(c)) making reference to Guideline 9 where a clear differentiation has been made between the type of due diligence requested in case of outsourcing to critical or important operational functions or activities *versus* in case of less-material outsourcing; - did not change the paragraph 27(d) (former paragraph 24(d)) as it considers that an assessment of conflict of interests should be performed in line to the requirement – for the undertaking – to be fully responsible for discharging all its obligations when outsourcing any function or activities (as stated in EIOPA system of governance paragraph 1.14);

Response to the public consultation question	EIOPA's comments
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	- streamlined the criteria contained in Guideline 7 striving to further align the factors to be taken into account when performing the assessment described by the Guideline to the ones requested by paragraph 31 of the EBA Guidelines on outsourcing. As a result of this review, some of the criteria previously foreseen by the Guideline were deleted. **EIOPA updated the Guidelines accordingly.**

Response to the public consultation question	EIOPA's comments
the cloud provider's server. If data is only transmitted for a very short period of time, e.g. 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.	
10. Is the content of 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.	**EIOPA partially agrees with the concerns raised by the respondent.** For this reason and to ensure a better inclusion of the principle of proportionality, EIOPA reviewed extensively the content of this Guideline by: 1) reducing the number of areas to be checked during the risk assessment; 2) enhancing the flexibility of application of the Guideline; 3) focusing the scope of application of the Guideline only on critical or important operational functions and activities outsourced. On the specific requests to amend elements of the Guidelines, EIOPA: - deleted former paragraph 28; - kept the requirement at former paragraph 29, being the information on the expected benefits and costs a possible metric of the significance of the provider, - For the cost benefit analysis a qualitative analysis can be performed. The wording has been clarified. - included the specification to assess the concentration risk at the level of the group; - kept and clarified the requirement of former paragraph 30(g) now transposed at paragraph 31(b)iv - reviewed the wording of former paragraph 30(h) It is important the decision making body is aware, in case of outsourcing of critical or important operational functions or activities, whether the cloud

Response to the public consultation question	EIOPA's comments
- 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 (e.g. 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	service provider has a market dominance. This is a useful information that the decision making body should weigh in the risk assessment to decide whether or not outsource to that specific cloud service provider the specific service. The Guidelines do not preclude the outsourcing to cloud service providers with market dominance. EIOPA clarified in the Guideline when a review of the risk assessment should be performed. **EIOPA updated the Guidelines accordingly.**

Response to the public consultation question	EIOPA's comments
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.	
11. 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, e.g. associated documentation regarding the data protection or service descriptions.	**EIOPA partially agrees with the concerns raised by the respondent.** <u>On Guideline 10 (contractual requirements)</u> EIOPA reviewed extensively the text of the Guideline to ensure a better inclusion of the principle of proportionality. In light of this, EIOPA: - reviewed the scope of application of the Guideline which will be applicable only in case of cloud outsourcing of critical or important operational functions or activities; - clarified the relationship between this Guideline and the requirements set by Directive 2009/138/EC and Commission Delegated Regulation (EU) No 2015/35 by eliminating the former paragraphs 36 and 37. Furthermore, bearing in mind the possible complexities of its implementation in case of misalignments between the content of this Guideline and of the one set by the EBA on the same subject, EIOPA further aligned the wording of this Guideline to the EBA requirements set by paragraph 75 of the EBA Guidelines on outsourcing. In light of this, on the specific requests to amend elements of the Guidelines, EIOPA: - agrees with the respondent being up to the contractual parties to consider mandatory insurance for the outsourced activities and whether this issue should be addressed in the outsourcing agreement. For this reason clarified the point in the Guideline; - to avoid unnecessary complexities in understanding how to apply the Guideline and to leverage on implementation already carried out by several cloud service providers to comply to the EBA Guidelines on the same subject, EIOPA kept the same wording as defined by the EBA Guidelines on data localisation and on performance target. The expression "written agreement" is the same used in the Guidelines on System of Governance and therefore it has been kept. EIOPA is aware that there might be more documents to describe the business relationship between an undertaking and its cloud service providers and that the contents of the Guideline 10 can be included in one or more of them.

Response to the public consultation question	EIOPA's comments
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.	On the possibility to organise a workshop with cloud service providers on these Guidelines, EIOPA will evaluate this possibility in 2020. <u>On Guideline 9 (due diligence)</u> The legal basis of that requirement are the Article 49 of Solvency II Directive, the article 274 (3) of Solvency II Delegated Regulation and paragraph 1.14 of the System of Governance Guidelines. On the possible confusion between the term "due diligence" used in these Guidelines and the one used at Article 256 of Commission Delegated Regulation (EU) No 2015/35, EIOPA is the opinion that there is no confusion and therefore made no changes. To ensure a better inclusion of the principle of proportionality, EIOPA reviewed the content of the Guideline. Particularly, EIOPA: - included a specific paragraph in the Guideline to specify that if an undertaking enters into a second agreement with a cloud service provider already assessed by that undertaking, the undertaking should determine, on a risk-based approach, whether a second due diligence is needed; - better distinguished between the due diligence to be performed on cloud service providers in case a critical or important operational function or activity is outsourced to them *versus* the due diligence on cloud service providers for less material outsourcing. In order to evaluate the suitability of the cloud service provider, an undertaking could use certificates based on international standards. These include but are not necessarily limited to International Safety Information Security Standard ISO / IEC 2700X of the International Organization for Standardization, C 5 Requirement Catalogue of the Federal Office for Information Security, Cloud Security Alliance standards. **EIOPA updated the Guidelines accordingly.**
12. 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, i.e. 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	**EIOPA agrees with the concerns raised by the respondent.** All the contractual requirements related to the outsourcing of non-critical, non-important operational functions to cloud service providers were deleted. **EIOPA updated the Guidelines accordingly.**

Response to the public consultation question	EIOPA's comments
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.	
13. Are the Guideline 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.	**EIOPA partially agrees with the concerns raised by the respondent.** EIOPA clarified the scope of application of Guideline 11, which will be applicable only in case of cloud outsourcing of critical or important operational functions or activities. Furthermore, in order to foster the development of European-wide standards in the area of auditing cloud services for financial institutions, EIOPA aligned the conditions to use third party certifications or audit reports to the ones set by the EBA Guidelines on outsourcing (paragraphs 92-93). These conditions include, in case of outsourcing of critical or important operational functions or activities to cloud service providers, the requirement for the undertakings to not rely solely on third-party certifications and reports over time. This means that undertakings should not simply assume that receiving a certificate or a report is enough assurance that the cloud service is being provided in accordance with their legal, regulatory and risk management obligations. If an undertaking elects to use third party certifications as audit tool, such undertaking should assess the adequacy of the information in these certifications against its own requirements and make follow-up enquiries to the cloud service providers if necessary (which might include the performance of on-site audits).

Response to the public consultation question	EIOPA's comments
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.	**EIOPA updated the Guidelines accordingly.**

Response to the public consultation question	EIOPA's comments
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 (e.g. 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	

Response to the public consultation question	EIOPA's comments
form of audit should be chosen depending on the identified risks and criticalities with regard to respective data and processes.	
14. 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	**EIOPA partially agrees with the concerns raised by the respondent.** On the point related to the common standards, EIOPA refers to the European Commission's work to develop a set of standardised contractual clauses as part of the FinTech Action Plan and the initiative to develop a SWIPO code of conduct[18]. On the point related to cloud security awareness, as reported in its report to answer the European commission FinTech Action Plan[19], EIOPA agrees with the respondent. Particularly, EIOPA recognises that the cloud service providers, in most cases, have built their infrastructure and service delivery models to support the most stringent security requirements at every level. Nonetheless, since cloud computing is a shared technology model – where different organisations are frequently responsible for implementing and managing different parts of the stack - from an operational perspective the security responsibilities are also distributed across the stack, and thus across the organisations involved. As a general principle, cloud customers (i.e. undertakings) are always responsible for what they do in the cloud and the cloud service providers are responsible for the cloud ('Shared responsibility framework"). One of the most important security considerations is knowing exactly who is responsible for what in any given cloud project. It's less important if any particular cloud provider offers a specific security control, as long as you know precisely what they do offer and how it works. For this reason, according to the Cloud Security Alliance Among the most significant security risks associated with cloud computing there is the tendency to bypass information and communication technology (ICT) departments and information officers[20]. On the content of the Guideline, EIOPA reviewed and streamlined it striving to further align the text to requirements set by paragraph 84 of the EBA Guidelines on outsourcing. As a result, several changes requested by the stakeholders have been included in the Guideline:

[18] Additional information on the SWIPO code of conduct initiative can be obtained at this link.

[19] The joint advice can be obtained at this link.

[20] The report published by EIOPA as answer to the European Commission FinTech Action plan can be obtained here

Response to the public consultation question	EIOPA's comments
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:"	- the reference to the definition of a data residency policy has been removed and substituted with a more principle based instruction; - the wording of former paragraph 50(g) (now, 49(i)) has not been changed. EIOPA assessed the Guidelines before and after the consultation and did not identify this as an area that would contradict the GDPR. - On the point on sub-outsourcing, EIOPA agrees with the respondent and clarified the Guideline. On the application of the principle of proportionality to this Guideline, EIOPA clarified its expectation. EIOPA would expect that the (re)insurance undertakings stay in control of their critical or important operational functions or activities (collectively "services" e.g. certain IT infrastructure, systems, environments, business applications, etc.) outsourced to cloud service providers. This operationally means that the undertakings monitor the performance of these services according to the SLAs defined with the providers and include them in the (wider) scope of monitoring of the entire undertaking's mission critical IT services. However, as reported under the EIOPA comments to respondent's answer to Question1, undertakings should be able to manage all of their risks when entering into an arrangement with third parties, including the operational risk of inappropriate or failing IT systems (soft- and hardware), and have to take appropriate business continuity and security measures. **EIOPA updated the Guidelines accordingly.**

Response to the public consultation question	EIOPA's comments
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.	
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", i.e. 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	**EIOPA agrees with the concerns raised by the respondent and updated the Guidelines accordingly** EIOPA reviewed extensively the content of the Guidelines to ensure their flexible and more proportionate application. On Guideline 13 (sub-outsourcing), EIOPA changed the title of the Guideline to "Sub-outsourcing of critical of important operational functions or activities" and clarified its contents. On Guideline 15 (Termination rights and exit strategies), EIOPA clarified the meaning of "sufficiently tested"

Response to the public consultation question	EIOPA's comments
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.	
16. 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. **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.	On the specific comments on Guideline 14 ("Monitoring and oversight of cloud outsourcing"), EIOPA avoided repetition of concepts/requirements included in other Guidelines. Moreover, EIOPA clarified that the main focus of monitoring should be the critical or important operational functions or activities outsourced to cloud service providers.
Annex Yes / No	
YES	

Fédération Française de l'Assurance, France

Response to the public consultation question	EIOPA Comments
1. Is the scope of application provided appropriate and sufficiently clear?	
No, please refer to our remarks above (the FFA's remarks are reported below). **General Comments** The FFA studied carefully the EIOPA consultation paper on the proposal for Guidelines on outsourcing to cloud service providers. The FFA thanks EIOPA for giving the possibility to comment on this proposal that really got our attention. First of all, regarding outsourcing and data protection, the FFA would like to precise that insurance companies have already to comply with very complete sets of rules which must remain the references (see for outsourcing: Solvency 2 regulation and for data protection: GDPR regulation). **We believe that all relevant texts regarding outsourcing or data protection should refer to Solvency 2 or GDPR and their terminology.** Having said that, proposing a formal framework regarding the specific issue of cloud outsourcing could be useful; there is an interest in formulating a specific approach to this technology which is becoming increasingly important for all areas of activities. Indeed, for insurance sector, giving clarification and transparency to market participants regarding cloud outsourcing arrangements could be useful. We believe that, at this point, the proposed approach seems difficult to consider taking into account: - the lack of proportionality and the systematic nature of the proposals, Cf; 1/ - the introduction of a new concept: "material outsourcing" which does not exist into Solvency regulation, Cf. 2/ - excessive burdens for insurance companies regarding contractual requirements, audit and control on cloud service providers, Cf. 3/ - a too short timeline, Cf. 4/ - insurance group specificities which are not taken into account, Cf.5/ Furthermore, the FFA does not understand why the proposed Guidelines are much more detailed than EBA Guidelines. Regarding the form and the general presentation of the document, it is difficult to understand which Guidelines are only applicable to material cloud	**EIOPA partially agrees with the concerns raised by the respondent.** On point 1/ Lack of proportionality/systematic nature of the proposals In case of outsourcing an undertaking has to ensure that it remains fully responsible for discharging all its obligations when outsourcing any function or activities (as stated in EIOPA system of governance paragraph 1.14). For the outsourcing of critical or important operational functions or activities, an undertaking must meet a number of requirements. In light of this, aiming at embedding the principle of proportionality and a risk-based approach, EIOPA streamlined the contents of the Guidelines, which are simpler and mainly focused on outsourcing of critical or important operational functions or activities to cloud service providers. However, some of the provisions contained in the Guidelines are still applicable also to outsourcing of non-critical, non-important operational functions or activities. On intra-group outsourcing, EIOPA agrees with the comment made by the FFA and, for this reason, made specific reference to the Guidelines on System of Governance. On point 2/ Lack of proportionality/systematic nature of the proposals EIOPA agrees with the concerns raised by the respondent, for this reason, on the basis of the feedback received and bearing in mind that one of the main purposes of these Guidelines is to provide clarity to the market participants, EIOPA decided to withdraw the use of the term "material outsourcing" sticking to the term "critical or important operational function and activity On point 3/Excessive burdens for insurance companies regarding contractual requirements, audit and control on cloud service providers - On the possibility to organise a workshop with cloud service providers on these Guidelines, EIOPA will evaluate this possibility in 2020; - On the possibility to develop a standardised set of contractual clauses, to foster supervisory convergence and market agility, EIOPA EIOPA refers to the European Commission's work to develop a set of standardised contractual clauses as part of the FinTech Action Plan and the initiative to develop a SWIPO code of conduct. - On the point related to the development of an ISO certificate for cloud service providers, competent authorities and EIOPA have no direct role in the oversight of service providers that do not fall within the scope of their action. There is no legal basis for introducing a certification for

Response to the public consultation question	EIOPA Comments
outsourcing arrangements and Guidelines which are also applicable to non-material cloud outsourcing arrangements. In this context, we would like to suggest a couple of key points to make EIOPA's proposals operational in order to facilitate relationships between insurers and cloud service providers. 1/ Lack of proportionality/systematic nature of the proposals First of all, the FFA would like to recall that, regarding outsourcing arrangements, the insurance sector has to comply with a very detailed and complete set of rules[21]. Furthermore, the FFA would like to precise that the use of cloud outsourcing is steadily increasing and involves in many cases non critical or important business activities of the insurance company. Obligations contained in the Guidelines regarding, documentation requirements, pre-outsourcing analysis, due diligence…concern all cloud outsourcing and involve disproportionate means, costs and extended deadlines. Therefore, the FFA believes that EIOPA should adopt a proportionated approach regarding cloud outsourcing arrangements which are not directly relevant to critical or important functions or activities (see solvency 2 regulation); **the scope of the Guidelines should be reviewed in order to exclude cloud outsourcing arrangements which are not directly relevant to critical or important functions or activities of the insurance company.** Furthermore, intra-group outsourcing should be taken into account: there are indeed fewer risks in this type of intra-group transactions and the principle of proportionality should encourage the introduction of lighter requirements (monitoring, pre-analysis, audit, exit clauses and documentation…). 2/ Introduction of a new concept: "material outsourcing" The introduction of a new, unclear term: "material outsourcing" adds a level of complexity and confusion. Indeed, Solvency II regulation (Directive 2009/138, delegated regulation 2015/35, EIOPA Guidelines on system of gouvernance-section11) only refers to "critical or important operational functions and activities".	'approved cloud service providers'. The responsibility for the selection of the cloud service providers lies with the undertaking. - On the suggestion related to the direct oversight of cloud service providers, EIOPA refers to the Joint Advice of the European Supervisory Authorities to the European Commission on the need for legislative improvements relating to ICT risk management requirements in the EU financial sector[22] On point 4/A too short timeline EIOPA moved the date of application to 1 January 2021 and prolonged the period for reviewing the existing arrangements to 31 December 2022. Moreover, in order to make the Guidelines more proportionate, a principle of risk-based review has been introduced (i.e. only contract related to critical and important operational functions should be amended, where needed. On point 5/Insurance group specificities which are not taken into account In addition to the clarification listed above, EIOPA specified that the entities subject to other sectoral supervisory requirements, which are part of a group, are excluded by the scope of application of these Guideline at solo level as they shall follow the sectoral specific regulatory requirements as well relevant guidance issued by the European Securities and Markets Authority and the European Banking Authority. Furthermore, EIOPA wishes to clarify that in case of groups and intra-group outsourcing where cloud infrastructure is used directly or as part of the sub-outsourcing chain, such arrangements also fall within the scope of these Guidelines. **EIOPA updated the Guidelines accordingly.**

21 See Solvency 2 Directive 2009/138, delegated regulation 2015/35, EIOPA's Guidelines on system of governance, RGPD 2016/679

22 The joint advice can be obtained at this link.

Response to the public consultation question	EIOPA Comments
EIOPA should use existing terms and concept in order to avoid any confusion or source of misunderstanding. The proposed Guidelines should refer to Solvency 2 regulation and delete the very confusing notion of "materiality". **These Guidelines should just focus on a "translation" or an interpretation of existing requirements (Solvency II Corpus regarding outsourcing) to a limited number of special aspects and issues related to cloud computing.** 3/Excessive burdens for insurance companies regarding contractual requirements, audit and control on cloud service providers 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). The FFA would like to stress that, in the context of its contractual relations with giant cloud providers it will be very difficult to impose contractual rules or audit rights. Therefore: - **the FFA strongly encourages EIOPA to engage with cloud service providers to ensure their willingness to adhere to all these very heavy requirements.** - **Regarding contractual relationships with cloud service providers, a solution could be to elaborate, at EU level, model clauses complying with competitions rules.** - Regarding multiple and disproportionate controls on cloud service providers**, it could be appropriate to elaborate an ISO certificate for these providers,** guaranteeing the continued compliance with high level safety requirements with which the insurers and other interested parties can trust. - If cloud providers where such a critical infrastructure, supervision of these actors could be as well envisaged. 4/ A too short timeline Insurance companies have complex structures, any change in their systems/process is usually very time consuming. That is why regarding proposed timeline to implement the Guidelines, an additional time period to comply with the requirements should be granted, the	

Response to the public consultation question	EIOPA Comments
proposed dates are too short, even if the FFA welcomes the flexibility proposed if the review of cloud outsourcing arrangements is not finalized by 1 July 2022. Indeed, these Guidelines will involve important contractual renegotiations, therefore the deadline of 1 July 2020 regarding new arrangements, which are already under negotiation, is too short for the correct application of final Guidelines published in January 2020. Regarding existing cloud outsourcing arrangements, an additional period should be granted to ensure that could outsourcing arrangements are compliant with the Guidelines. 5/ Insurance group specificities which are not taken into account The French market have a significant number of big actors (8 International Active Groups in the ICS framework); most of them have a holding company acting on behalf of its subsidiary. EIOPA does not take adequate account insurance groups with a holding acting on behalf of its subsidiaries. This particular issue should be addressed in the proposed Guidelines.	
2. Is the set of definitions provided appropriate and sufficiently clear?	
Generally speaking, the FFA does not understand why the number of definitions of EIOPA Guidelines is far more important than definitions listed in EBA Guidelines. **As a general principle, all the definitions contained into the Guidelines should absolutely refer to those included into Solvency 2 regulation.** - The definition of "*function*" should be deleted, recital 31 and art. 13.29 of Solvency 2 directive already contains a definition of function[23]; the Guidelines should only refer to the Solvency 2 definition. - The definition of "material outsourcing" should be removed or only refers to "*outsourcing of critical or important operational functions or activities as defined in Solvency 2 regulation*". - The definition of "*service provider*": is not clear. What is meant by "*performing an outsourced process, service or activity, or parts thereof,*	**EIOPA partially agrees with the concerns raised by the respondent.** Function, in order to avoid the possible confusion with Article 13(29) of Solvency II Directive, EIOPA decided to delete the definition. The definition has been deleted. Material outsourcing, on the basis of the feedback received and bearing in mind that one of the main purposes of these Guidelines is to provide clarity to the market participants, EIOPA decided to withdraw the use of the term "material outsourcing" sticking to the term "critical or important operational function and activity". The definition has been deleted Service provider the definition has been clarified. Cloud service provider, the definition has been clarified.

[23] "*A function is an administrative capacity to undertake particular governance tasks. The identification of a particular function does not prevent the undertaking from freely deciding how to organize that function in practice save where otherwise specified in this Directive. This should not lead to unduly burdensome requirements because account should be taken of the nature, scale and complexity of the operations of the undertaking. It should therefore be possible for those functions to be staffed by own staff, to rely on advice from outside experts or to be outsourced to experts within the limits set by this Directive*." And "'function: *within a system of governance, means an internal capacity to undertake practical tasks; a system of governance includes the risk-management function, the compliance function, the internal audit function and the actuarial function*;

Response to the public consultation question	EIOPA Comments
under an outsourcing arrangement"? Does that include third parties which are not cloud service providers but rely significantly on cloud infrastructure to deliver their services, as well as cloud brokers? - The definition of "*cloud service provider*" is far too broad and would force insurance companies to take into account all IT service providers. What is meant by third party who "*rely significantly on cloud service providers to deliver their services*"? - The definition of "*cloud broker*" should be deleted to the extent that the term is not used anymore in the text of the Guidelines. - The definition of "*significant sub-outsourcer*" is not clear, it is too broad. - The definition of cloud services should insist on the opposition between the cloud and local storage: this kind of definition could be proposed: "*Services provided through a cloud, i. e. a set of computer resources (e. g. networks, servers, storage, applications) that are exclusively accessible remotely and allow computer processing without local storage of data or applications and without the service customer receiving dedicated computer resources*." - Public Cloud: this definition should be precised - Private Cloud: this definition should be precised	Cloud broker, as the concept of cloud broker is not used in the Guidelines, EIOPA decided to delete the definition. The definition has been deleted. Significant sub-outsourcer on the basis of the feedback received and in order to have market consistency the definition has been deleted Cloud services, in order to have market consistency the definition has been kept aligned to the one used in the EBA Guidelines on outsourcing. No changes have been made. Public cloud, in order to have market consistency the definition has been kept aligned to the one used in the EBA Guidelines on outsourcing. No changes have been made. Private cloud, in order to have market consistency the definition has been kept aligned to the one used in the EBA Guidelines on outsourcing. No changes have been made. **EIOPA updated the Guidelines accordingly.**
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, please refer to our remarks above.	EIOPA's comments at question 1.
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?	
For us, the Guideline is quite unclear; examples/clear criteria should be given of what should not be considered as outsourcing to cloud service providers, as many companies providing IT services rely on clouds for their own activity. Indeed, there are many services that should never be expected to be undertaken by an undertaking itself (e.g. emails system, procurement of storage space/server capacity) and can be classified as a mere purchasing of services rather than as actual outsourcing of the same. Conclusion: only the functions and activities which are deemed critical and important for the activities of the undertaking under Solvency 2 rules should be covered by the Guidelines and only where actually outsourced to a cloud service provider.	**EIOPA partially agrees with the concerns raised by the respondent.** The determination of whether (or not) the purchase of cloud services fall into the scope of outsourcing is paramount to a successful and coherent application of these Guidelines. The assessment to this application is responsibility of the undertakings and should be carried out by applying the criteria provided in Guideline 1 and in the regulatory obligations listed in the introduction of these Guidelines. There are two type of arrangements with third parties service providers: 1) Services which are not outsourcing and 2) Services which are outsourcing. Among the services which are outsourcing there is a distinction between:

Response to the public consultation question	EIOPA Comments
	- outsourcing of critical or important operational functions (which includes, but is not limited to, insurance and reinsurance processes and activities, functions as defined by Solvency II art. 13(29), provisioning of on-going day to day systems maintenance or support, investment of assets or portfolio management, etc.) - outsourcing of non-critical, non-important operational functions (i.e. less material). As reported above, an undertaking has to ensure that it remains fully responsible for discharging all its obligations when outsourcing any function or activities (as stated in EIOPA System of Governance paragraph 1.14). For the outsourcing of critical or important operational functions or activities, an undertaking must meet certain requirements. When an undertaking purchases cloud services, it has to perform the same type of assessment due in case of "general outsourcing", namely 1) understand whether the purchase of cloud services is outsourcing or not; 2) if it classifies as outsourcing, understand whether the outsourced function is critical or important; 3) on critical or important operational functions or activities, perform a detailed risk assessment on the operational function/activity to be outsourced and a detailed due diligence on the service provider; 4) On all the less material outsourcing, in order to fulfil its responsibility obligation (as stated above), a risk assessment and a due diligence (of higher level compared to the previous point) are to be performed. Furthermore, notwithstanding the results of the assessment of whether the provisioning of cloud services falls under the definition of "outsourcing", as part of their internal control system, on a risk and proportionate way, the undertaking should identify, measure, monitor, manage and report risks caused by arrangements with third parties regardless whether or not those third parties are cloud service providers.
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?	
For the FFA, there is no need to elaborate a Guideline regarding written policy which already exists with Solvency 2 requirements regarding outsourcing. Conclusion: cloud outsourcing arrangements (related to critical or important function or activity) should be integrated into the overall outsourcing process to ensure a consistent governance.	**EIOPA partially agrees with the concerns raised by the respondent.** EIOPA has decided to keep the Guideline clarifying its application. For this reason, as the Solvency II principles on outsourcing are still valid for cloud, with reference to the update of internal policies and procedures, multiple solutions are at disposal for undertakings: 1) development – where needed – of a dedicated cloud outsourcing policy;

Response to the public consultation question	EIOPA Comments
	2) complement - where needed – the undertaking outsourcing policy and the other relevant internal policies (for example the information security policy) to take into account the specificities of outsourcing to cloud service providers; and 3) if the undertaking current policies cover the elements described in these Guidelines, there is no need to update. **EIOPA updated the Guidelines accordingly.**
5b. Is the Guideline on written policy consistent to the market best practices on defining the policy for general outsourcing?	
See answer above	NA
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?	
The notification requirement should be limited to cloud outsourcing arrangements involving critical or important function or activity. The list of information to be notified should be in line with notification required by Solvency 2 regulation regarding outsourcing (only for critical or important function or activity). Practical details regarding this notification's procedure should be decided at national supervisory authority level. Conclusion: the notification of a cloud outsourcing agreement to the national supervisory authority should follow the same rules and be in the same form than that provided for any other Solvency 2 outsourcing arrangement.	**EIOPA partially agrees with the concerns raised by the respondent.** The content of Guideline 4 which is related only to outsourcing of critical or important operational functions or activities has been streamlined by: (a) removing the requirement to present a draft copy of the outsourcing agreement (b) aligning the requirements to the EBA requirements set by paragraph 54 of the EBA Guidelines on outsourcing to ensure market consistency for outsourcing to cloud service providers. **EIOPA updated the Guidelines accordingly.**
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?	
For a sound governance, the FFA is not opposed in principle to list cloud outsourcing arrangements regarding critical or important functions but the Guideline gives too much details; the form and the location of this kind of information should be taken by the insurance company. Indeed, Insurance companies should have more flexibility with regards to the oversight of cloud outsourcing arrangements. The FFA would like to stress the difficulty of maintaining and updating a register regarding cloud service arrangements, because of the pace of change regarding cloud outsourcing offers and the number of departments involved in the process.	**EIOPA partially agrees with the concerns raised by the respondent.** EIOPA has streamlined the content of the Guideline 5 by removing the requirements for keeping a register and requiring the undertaking to record information of their cloud outsourcing arrangements. Furthermore, EIOPA has defined, as minimum requirement, a set information to be recorded only for critical or important operational functions outsourced to cloud service providers. This set of information is aligned to the one required by the EBA Guidelines on Outsourcing. For outsourcing to cloud service providers on non-critical non-important operational functions or activities, the level of detail of information to be recorded should be determined by the undertakings on a risk-based approach.

Response to the public consultation question	EIOPA Comments
Furthermore, the FFA does not see the need of a special register for cloud outsourcing arrangements. Cloud out-sourcing arrangements should be mentioned in the general outsourcing register/document. Finally, the requested documents regarding the description of the services used and the data stored raise confidentiality concerns; communicate these kinds of highly confidential information outside the company presents a real risk. Conclusion: there is no need for a special register regarding cloud outsourcing; should there be a requirement for a separate register, insurance companies should be let free to elect the deemed appropriate mean/tool for the oversight of their cloud outsourcing arrangements and it should be limited to cloud outsourcing arrangements relating to critical or important function or activity and the information to be populated in such a register should be limited to what is strictly necessary to ensure monitoring, all other information being in any case duly recorded in the contract itself.	These Guidelines do not preclude the undertakings to keep record of the information on their cloud outsourcing arrangements in a "general outsourcing register/document". EIOPA will undertake a broader and comprehensive discussion on how to document discussion on how document outsourcing arrangements when reviewing the System of Governance Guideline. On the risks of breaching confidentiality arrangements with third parties when sharing confidential information with the national supervisory authority, EIOPA would like to underline that the all persons who are working or have worked for supervisory authorities are bound by the obligation of professional secrecy as disciplined by article 64 of Solvency II Directive. **EIOPA updated the Guidelines accordingly.**
7b. What can be other approaches to ensure a proper and sound holistic oversight of cloud outsourcing?	
See answer above	NA
8. Are the documentation requirements appropriate and sufficiently clear?	
The documentation/information requirements listed under paragraph 23 appear unnecessarily stringent and burdensome, in particular: - 23(a) duplicates the notification; - 23(c) unnecessary, already provided for in the undertaking policy (should be the same for all arrangements entered into by a given undertaking); - 23(d) interest of having estimate cost in the register unclear; - 23(f) the mentions regarding sub outsourcers should be incorporated in the contract itself not in a register; - At paragraph 23(g), please clarify what is meant by "time critical". - As regards paragraph 23(i), the required level of detail regarding the description of the undertaking monitoring of the cloud outsourced activities is too specific. Considering that the number of resources and their skills may vary from time to time, it would be too burdensome to regularly update the register in that regard.	**EIOPA partially agrees with the concerns raised by the respondent.** In particular: - former paragraph 23(a) (Paragraph 24(a)) was kept as undertakings should record the information notified to the supervisory authority; - the content of former paragraph 23(c) (Paragraph 24(c)) was clarified; - being the information on budget costs a possible metric of the significance of the provider, kept the requirement to record it. Moreover, in order to clarify the purpose, EIOPA aligned the wording to the one used by the EBA in its Guidelines on outsourcing; - the content of former paragraph 23(c) (Paragraph 24(c)) was clarified; - on the former paragraph 23(g) (Paragraph 24(h), assessment of criticality of processes, applications and systems should be performed by each individual undertaking, for example as part of the definition of its own business continuity objectives during their Business Impact Analysis. Therefore, EIOPA is the opinion that the definition of "time critical" applications should be defined by each single undertaking; - the requirement at former paragraph 23 (h) has been removed the requirement to record a description of the undertaking monitoring of the cloud outsourcing activities. **EIOPA updated the Guidelines accordingly.**

Response to the public consultation question	EIOPA Comments
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, as explained above, EIOPA should absolutely delete this new confusing concept and stay with Solvency 2 concept regarding important or critical functions or activities. The introduction of a new, unclear term: "material outsourcing" adds a level of complexity and confusion. Indeed, Solvency II regulation (Directive 2009/138, delegated regulation 2015/35, EIOPA Guidelines on system of gouvernance-section11) only refers to "critical or important operational functions and activities". EIOPA should use existing terms and concept in order to avoid any confusion or source of misunderstanding. The proposed Guidelines should refer to Solvency 2 regulation and delete the very confusing notion of "materiality". **These Guidelines should just focus on a "translation" or an interpretation of existing requirements (Solvency II Corpus regarding outsourcing) to a limited number of special aspects and issues related to cloud computing.** We believe that cloud outsourcing is "only" another form of outsourcing and therefore should follow the same logic as "traditional" outsourcing (as referenced in Solvency 2). There is no reason to develop for cloud outsourcing arrangements more stringent rules than for other outsourcing arrangements.	**EIOPA partially agrees with the concerns raised by the respondent.** On the use of the term "material" instead of the term "critical or important", as reported above, bearing in mind that one of the main purposes of these Guidelines is to provide clarity to the market participants, EIOPA decided to withdraw the use of the term "material outsourcing" sticking to the term "critical or important operational function and activity". **EIOPA updated the Guidelines accordingly.**
10. Is the content of Guideline on risk assessment of cloud outsourcing appropriate and sufficiently clear?	
- We understand that Paragraph 28 apply to all cloud outsourcing, 29 only for material outsourcing, what about paragraph 30? - Please provide examples of "high-severity, operational risks events" in the context of cloud outsourcing, as referred to in paragraph 28. - In paragraph 30(g)(i), "the laws in force" is too broad, there should be limitative list of laws to be taken into account within the risk assessment (e.g. laws on data protection). - The risk assessment methodology should not so differ, subject to the very specificities of cloud services, from that applicable to the outsourcing of important or critical functions or activities. - This Guideline should also take into account the impact of events affecting the cloud service provider.	**EIOPA partially agrees with the concerns raised by the respondent.** EIOPA reviewed extensively the content of this Guideline to ensure a better inclusion of the principle of proportionality by: (1) reducing the number of areas to be checked during the risk assessment; (2) focusing the scope of application of the Guideline only on critical or important operational functions and activities outsourced. On the points raised by the respondent: - The new paragraphs 30 and 32 will apply to all outsourcing to cloud service providers the new paragraph 31 applies only to critical or important operational functions or activities; - The point on performing scenario analysis taking into account "high severity operational risk events" has been removed;

Response to the public consultation question	EIOPA Comments
Conclusion: risk assessment regarding cloud outsourcing arrangements is already covered by the risk assessment conducted as part of the general outsourcing arrangements. For the FFA the proposed list of elements to be verified by the insurance company should be indicative and should not be binding.	- On the point related to the laws in force, EIOPA kept and clarified the requirement of former paragraph 30(g) now at paragraph 31(b)iv - EIOPA, in principle, agrees with the fact that the risk assessment methodology should not differ from the one applicable to outsourcing (not to cloud service providers) of critical or important operational functions or activities and that should take into account the impacts of events affecting the cloud service providers. **EIOPA updated the Guidelines accordingly**
11. Are the contractual requirements for material outsourcing appropriate and sufficiently clear?	
Generally speaking, the FFA would like to stress that in most cases, the service provider offers a standardized and packaged offer, which is identical for all its clients, and which can hardly be adapted and customized for a specific client. Furthermore, art. 274 Paragraph 4 delegated act 2015/35 regarding general sub-outsourcing already describes (only for outsourcing of critical or important operational functions or activities) the content of the written agreement between the undertaking and the service provider in exhaustive detail. Nonetheless, Guideline 10 (Paragraph 35) sets out a number of new requirements ("in addition to the set of requirements defined by Article 274…"). We see no benefit in the additional requirements. Finally, to our knowledge, EBA Guidelines do not contain any list of contractual requirements… - Regarding 35. The use of such terms as "at least" is confusing. - Regarding 35.d ("*the parties' financial obligations including the cloud services pricing model*") could be a problem: currently, major cloud service providers only propose on-line price models; therefore the Guidelines should absolutely refer to the price model available on-line. - 35.i monitoring cloud service provider cannot be "on an ongoing basis", the term "regular" should be preferred. - In paragraph 35 j, please provide examples of quantitative and qualitative performance targets that are directly measurable by the undertaking. - Regarding 35.l of the Guidelines ("*whether the cloud service provider should take mandatory insurance against certain risks and, if applicable, the level of insurance cover requested*") for instance, it is up to the contractual parties to consider insurance coverage for the	**EIOPA disagrees with the concerns raised by the respondent.** However EIOPA reviewed extensively the text of the Guideline to ensure a better inclusion of the principle of proportionality. In light of this, EIOPA: (1) reviewed the scope of application of the Guideline which will be applicable only in case of cloud outsourcing of critical or important operational functions or activities; (2) clarified the relationship between this Guideline and the requirements set by Directive 2009/138/EC and Commission Delegated Regulation (EU) No 2015/35 by eliminating the former paragraphs 36 and 37. Furthermore, bearing in mind the possible complexities of its implementation in case of misalignments between the content of this Guideline and of the one set by the EBA on the same subject, EIOPA further aligned the wording of this Guideline to the EBA requirements set by paragraph 75 of the EBA Guidelines on outsourcing. In light of this, on the specific requests to amend elements of the Guidelines, EIOPA: - removed the wording "at least"; - removed the reference to the "cloud pricing model" to avoid possible confusion; - kept the right, for an undertaking, to monitor on an "on-going basis" its cloud service provider; - clarified the point on monitoring of performance targets, - agrees with the respondent being up to the contractual parties to consider mandatory insurance for the outsourced activities and whether this issue should be addressed in the outsourcing agreement. For this reason clarified the point in the Guideline; - to avoid unnecessary complexities in understanding how to apply the Guideline and to leverage on implementation already carried out by several cloud service providers to comply to the EBA Guidelines on the

Response to the public consultation question	EIOPA Comments
outsourced activities and whether this issue should be addressed in the outsourcing agreement. This should remain so… - Regarding 35.n: this provision will be difficult to apply, in case of bankruptcy the treatment of contractual debts and credit depends on legal provisions or on liquidator/court administrator's decision. Conclusion: for all the reasons explained above, the Guideline 10 could be removed. Regarding contractual relationships with cloud service providers, a solution could be to elaborate, at EU level, model clauses complying with competitions rules. Indeed, insurance undertakings suffer from a weak bargaining power compared to giant cloud service providers, models clauses compulsory for contracting parties could be the solution	same subject, EIOPA kept the same wording as defined by the EBA Guidelines on data localisation and on performance target; - on the point related to former paragraph 35(n), making reference to the undertaking's data (and not to their debts and credits), the provision has been kept. Furthermore, as reported above at EIOPA's comments to FFA question 1, EIOPA refers to the European Commission's work to develop a set of standardised contractual clauses as part of the FinTech Action Plan. **EIOPA updated the Guidelines accordingly.**
12. Are the criteria provided to set the contractual requirements for non-material outsourcing appropriate and sufficiently clear?	
There should be no contractual requirements for non-material cloud outsourcing arrangements, which should not fall within the scope of these Guidelines.	**EIOPA partially agrees with the concerns raised by the respondent.** All the contractual requirements related to the outsourcing of non-critical, non-important operational functions to cloud service providers were deleted. **EIOPA updated the Guidelines accordingly.**
13. Are the Guideline on access and audit rights appropriate and sufficiently clear	
Many questions arise from Guideline 11 - Regarding these pooled audits, it is a good idea which must be further explored; however, cumulative requirements in 45 seem difficult to meet. - Please clarify paragraph 45(a). To which audit plan are you referring to? - In paragraph 45(b), the use of both "i.e." and "etc." makes it unclear whether the list of systems in brackets is limitative or not. Also, it refers to "systems" and "key controls", while paragraph 45(d) refers to "key systems and controls". Please correct this inconsistency and clarify the notions of key systems and controls. - In paragraph 45(c), "thoroughly" should be removed. Paragraph 45(c) should not amount to requiring a thorough audit of audit reports.	**EIOPA partially agrees with the concerns raised by the respondent.** In the final review of the Guidelines, aiming at fostering the development of European-wide standards in the area of auditing cloud services for financial institutions, EIOPA aligned the conditions to use third party certifications or audit reports to the ones set by EBA Guidelines on outsourcing (paragraphs 92-93). In light of this, on the specific requests to amend elements of the Guidelines, EIOPA: - On pooled audits confirms that the requirements set by paragraph 43 (former paragraph 45) are to be applied only if undertakings make use of third party certifications or internal audit reports (i.e. not in case of pooled audits); - Deleted the former paragraph 45(a) as result of FFA comment, as the audit plan is embedded into the audit plan of the undertaking; - Clarified the inconsistencies at former paragraphs 45(b) and (d) as general point, key systems are those considered business critical by the undertaking for example, following a business continuity analysis or an IT security assessment;

Response to the public consultation question	EIOPA Comments
- In paragraph 45(d), it is unduly burdensome to require undertakings to ensure that key systems and controls are covered in future versions of the certification or audit report. Undertakings should only ensure that key systems and controls are covered in the scope of the certification or audit report at the time they are using it as an audit method. - In paragraph 45(e), what is meant by "rotation of the certifying or auditing company"? - In paragraph 45 (g), difficult to apply, regarding most of cloud outsourcing arrangements, the service provider offers a standardized and packaged offer, which is absolutely identical for all its clients, and which can hardly be adapted and customized for a specific client (including audit aspects). - In paragraph 45(h), please clarify the extent of on-site audits in the context of cloud outsourcing, bearing in mind that the full rights to access and audit for outsourcing undertakings is difficult to implement in view of highly standardized services and contracts, the limited negotiation power of outsourcing undertakings, the risk these rights pose to the cloud environment of other clients of the cloud service provider, and the risk and operational implications for the cloud service provider as a whole. - In paragraph 48, please clarify the requirement on "the appropriate skills and knowledge". - How to measure satisfaction as referred to in paragraphs 45(a), 45(e) and 45(f)? - Please clarify that paragraphs 43 to 45 apply to both access and audit rights (not just audit). E.g. paragraph 43 should start with "If the exercise of access or audit rights, or the use of certain audit techniques…" <u>Conclusion</u>: the FFA would like to stress the difficulty of gaining acceptance for these access and audit rights (not least for reasons of confidentiality). In practice, it is common contractual practice for service providers to provide a limitation on the number of audit rights per year: is such as limitation	- Kept the word "thoroughly"; - Kept the requirement at former paragraph 45(d) (current paragraph 43(d)); - For "rotation of the certifying or audit company" it is meant the practice applied for rotation of the certifying or audit company for example number of years or number of mandate renewals; - should assess the these certifications against their own requirements and make follow-up enquiries to the cloud service providers if necessary (which might include the performance of on-site audits; - on former paragraph 45(g) and (h) (currently paragraphs 43 (f) and (g)), it is worth to mention that if an undertaking elects to use third party certifications as audit tool, such undertaking should assess the adequacy of the information in these certifications against its own requirements and make follow-up enquiries to the cloud service providers if necessary (which might include the performance of on-site audits or to enlarge the scope of the audit or the certification); - On the point related to former paragraph 45(h), EIOPA clarified the extent of on-site audits in the context of cloud outsourcing at Guideline 10 and 11 - on the question on how to measure satisfaction at paragraphs 41 (a), (e) and (f), EIOPA is the opinion that, in this context, the satisfaction should be assessed by each undertaking against its own risk appetite (e.g. the scope of the reports is considered appropriate by either the Internal Audit, Security, or Risk Management of the undertaking, the rotation of the certifying entity is compliant to the standard set by the undertaking/applicable law if any, the standards used by the certifying entity are the same or aligned to the ones used by the undertaking or after an assessment considered adequate). On the question of imposing a limitation on a number of audits per year, in case of outsourcing of critical or important functions, in principle, such limitation could consist in an impediment to the right of access and audits. However, applying a risk based approach, if the maximum number of audits allowed per year is sufficiently large (for example 4/5 per year), such limitation should not be considered as an impediment to the right of access and audits. In this last case, a crucial role is represented by the scope of audit. On the reliability of third parties certification, as reported above, undertakings can use them. However, they should not simply assume that receiving a certificate or a report is enough assurance that the cloud service is being provided in accordance with their legal, regulatory and risk management obligations. If an undertaking elects to use third party certifications as audit tool, such undertaking should assess the adequacy of the information in these

Response to the public consultation question	EIOPA Comments
considered an impediment to the rights of access and audit as per paragraph 39? As said before, cloud service providers could comply with an ISO or SOC (Service Organization Control) certification guaranteeing the continued compliance with high level safety requirements with which the insurers and other interested parties can trust.	certifications against its own requirements and make follow-up enquiries to the cloud service providers if necessary (which might include the performance of on-site audits or by request to enlarge the scope of the certification). **EIOPA updated the Guidelines accordingly.**
14. Are the provisions set by this Guideline for security of data and systems appropriate and sufficiently clear?	
Regarding data protection requirements, insurance sector has already to comply with GDPR regulation, which must remain the reference. Ongoing monitoring appears extremely stringent, or even possible to achieve. Insurance undertakings have already developed a PAS (Plan d'Assurance Qualité) annexed to the cloud agreement. At 50 (d), such proposal goes too far because of including the sub-outsourcers. At paragraph 50(g), please clarify how, and at which frequency, the undertaking should monitor the level of fulfillment of the requirements relating to the efficiency of control mechanisms implemented by the cloud service provider and its significant sub-outsourcers. Also, such monitoring should be limited to the cloud service provider as it is the cloud service provider's responsibility to monitor its sub-outsourcers. Conclusion: the FFA is in the opinion that these obligations must be borne by cloud service providers. As said before a solution could be to elaborate an ISO certificate for these providers, guaranteeing the respect of a high level safety requirements regarding security data and systems.	**EIOPA partially agrees with the concerns raised by the respondent.** EIOPA assessed the Guidelines before and after the consultation and did not identify this as an area that would contradict the GDPR. On the specific requests to amend or clarify specific elements of the Guidelines: - EIOPA streamlined the content of former paragraphs 50(d) and 50(g) (now paragraphs 49(f) and 49(i); - on the point related to the frequency of monitoring of the level of fulfilment of the requirements relating to the effectiveness and efficiency of control mechanisms implemented by the cloud service provider that would mitigate the risks related to the provided services, EIOPA agrees with the FFA that it is responsibility of the cloud service providers to monitor their outsourcers (sub-outsourcers for the undertakings). For the permitted sub-outsourcing of critical or important operational functions or activities (or part thereof), the undertaking should agree with the cloud service provider the elements specified in Guideline 13. The undertaking should be able to regularly monitor its cloud outsourcers on a risk based approach. **EIOPA updated the Guidelines accordingly.**
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.	
As a general principle it seems excessive to apply, beyond what is required from the very cloud services specificities, more stringent governance rules to the cloud outsourcing process than those required to be complied with for the outsourcing of key functions. Undertakings should be given some flexibility in the way they follow-up on and monitor, in compliance with Solvency 2 requirements, their Solvency 2 outsourcing arrangements. In the future a wide range of tools may become	**EIOPA partially agrees with the concerns raised by the respondent and updated the Guidelines accordingly.**

Response to the public consultation question	EIOPA Comments
available which would render the suggested "register" obsolete. Furthermore, the register proposed in the Guidelines and the information requested to be populated therein appear in practice hardly manageable for the undertakings considering, in particular, the number of contributors the ongoing update of such a register would involve without clear added-value for the undertakings as long as they keep strict record of their arrangements and have tools in place to duly monitor the various aspects of the arrangements in force. Conclusion: As explained in our general comments, the Guidelines suffer from a lack of proportionality; the best way to ensure proportionality is to restrict the scope of the Guidelines to cloud service arrangements regarding critical or important function or activity and stay in line with Solvency 2 requirements regarding outsourcing arrangements.	
16. Do you have any comments on the impact assessment?	
On Guideline 13 "Sub-Outsourcing" For the FFA, it should be a general rule: all sub-outsourcing arrangements are prohibited except those which are explicitly authorized by the insurance company, paragraph 53 should be amended accordingly. Furthermore, it is impossible for an insurance company to control all sub-outsourcers; the control should be restricted to outsourcer who are contractually bound to the insurance company; sub-outsourcers must be controlled by the cloud service provider. One possibility could be, for the insurer, to ask for the own outsourcing policy of the cloud service provider.	**EIOPA partially agrees with the concerns raised by the respondent and updated the Guidelines accordingly.**
Annex Y/N	
YES	

Dutch Association of Insurers, the Netherlands

Response to the public consultation question	EIOPA Comments
1. Is the scope of application provided appropriate and sufficiently clear?	
General remarks We think that these Guidelines could be beneficial for the position of insurance companies toward cloud services providers. We agree that cloud should be part of the digital transformation process, an enabler and a way to optimize IT expenses. Cloud helps to be flexible and scale when needed. New products and services will be more and more cloud based. Please keep in mind that there are also EBA Guidelines on Outsourcing (EBA/CP/2018/11). This shouldn't be contradictory. We support the need for an exit strategy and exit support in the contract with cloud outsourcing partners. However due to the nature of modern cloud services (e.g. SAAS and PAAS services), a detailed exit plan, with all activities, roles and responsibilities, which should be tested is often not feasible. The SAAS and PAAS services are developing rapidly, including potential alternatives to be used in case of an exit. We question whether there is a legal basis for requirements on non-material outsourcing. In our opinion there is no Solvency II requirement to maintain a register of non-material cloud outsourcing arrangements or to provide information about that to the supervisory authorities. If a company decides to do that, it should be on a voluntary basis. As there is no legal basis there is no need to include non-material outsourcing in the scope of these Guidelines. We advise to leave non-material outsourcing out of the scope. So there is no need for a register with respect to non-material outsourcing. Also there is no need for additional requirements. Item 2 of the Introduction states the Guidelines apply to entities which are part of the group (art. 212(1) Directive 2009/138/EC). Although the reasoning for applying the Guidelines to group entities is understandable, by doing so the supervisory tasks of EIOPA are extended to asset management and banks. The applicability of the Guidelines are extended without realising that there might already be Guidelines published by the relevant supervisory authority or the Guidelines might even conflict with Guidelines published by the relevant supervisory authority.	**EIOPA noted the concerns raised by the respondent.** In case of outsourcing, an undertaking has to ensure that it remains fully responsible for discharging all its obligations when outsourcing any function or activities (as stated in EIOPA system of governance paragraph 1.14). For the outsourcing of critical or important operational functions or activities, an undertaking must meet a number of requirements. In light of this, aiming at embedding the principle of proportionality and a risk-based approach, EIOPA streamlined the contents of the Guidelines, which are simpler and mainly focusing on outsourcing of critical or important operational functions or activities to cloud service providers. However, some of the provisions are applicable also to outsourcing of non-critical, non-important operational functions or activities. On the point related to the 'exit plan', EIOPA wishes to specify that an undertaking should have an exit strategy from cloud services (including if they are SAAS and PAAS) in case they are related to critical or important operational functions. EIOPA recognises that the type of exit strategies and plans may vary depending from the service provided by the service provider. EIOPA clarified the point by inserting some examples in paragraph 55(a) (former paragraph 60(a)). On the point related to the application of the Guidelines at solo level by group subsidiaries belonging to other financial sectors (for example investment management companies licensed under the Undertakings for Collective Investments in Transferrable Securities (UCITS) Directive or Alternative Investment Fund Management Directive (AIFMD), EIOPA welcomed the comments and clarified the point in the text of the Guidelines in paragraph 4.
2. Is the set of definitions provided appropriate and sufficiently clear?	

Response to the public consultation question	EIOPA Comments
No. In our view this is not the case for alignment (and because of that also not for the scope) with Solvency II. This makes it more complicated. Also a sub-outsourcer within insurers could also be defined as sub-contractor. The meaning is the same. We would due to the ambiguous definition of Cloud services also state IAAS, PAAS, SAAS. Material influence on a process can be because of a small, But significant dependency (tight coupling) on a service.	**EIOPA agrees with the concerns raised by the respondent.** On the definition of Material outsourcing, on the basis of the feedback received and bearing in mind that one of the main purposes of these Guidelines is to provide clarity to the market participants, EIOPA decided to withdraw the use of the term "material outsourcing" sticking to the term "critical or important operational function and activity". The definition has been deleted On the analogy between sub-outsourcer and sub-contractor, EIOPA agrees with the Dutch Association of Insurers that the meaning is the same. On the definition of Cloud services, EIOPA kept the definition as provided by the draft Guidelines to be consistent with the definition set by the EBA in its Guidelines on outsourcing. However, EIOPA removed the reference to the cloud service models (SaaS, IaaS and PaaS) and the related definitions and replaced this text with a more generic reference to 'cloud service models'. **EIOPA updated the Guidelines accordingly**
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?	
Yes, however we suggest EIOPA to contact/inform cloud providers about these Guidelines to increase their willingness to cooperate to amend existing arrangements. Concept of Guidelines (legally) does not match with a fixed deadline for implementation. One can/should follow these Guidelines where possible and applicable, but Guidelines shouldn't force insurers to be fully compliant (in all running and new contracts) per a certain date. Where and when applicable insurers may change our policies/processes in relation to outsourcing (to the cloud).	**EIOPA noted the concerns raised by the respondent.** On the possibility to liaise with cloud service providers on these Guidelines, in 2020, EIOPA will evaluate the possibility to organise a workshop with cloud service providers on these Guidelines. EIOPA decided to set a deadline for the application of the Guidelines in order to achieve their aim: (a) provide clarification and transparency to market participants avoiding potential regulatory arbitrages; (b) foster supervisory convergence regarding the expectations and processes applicable in relation to cloud outsourcing
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, the Guideline first makes a distinction between outsourcing and non-outsourcing. Subsequently, only for outsourcing a materiality assessment needs to place. We propose to integrate these (Guideline 1 and Guideline 7). We would appreciate further clarification for Material outsourcing only. Non-material outsourcing should be out of the scope	**EIOPA partially agrees with the concerns raised by the respondent.** EIOPA has decided not to merge Guideline 1 and Guideline 7. However, EIOPA agrees with the respondent on the fact that only on outsourcing, an undertaking should perform an assessment on whether the operational function or activity outsourced is a critical or important.

Response to the public consultation question	EIOPA Comments
It is stated that every cloud service should be seen as outsourcing: ''as a rule, outsourcing should be assumed''. Assuming that every cloud service is considered outsourcing is rather farfetched. The majority of cloud services are plain simple and cheap services that are bought off the shelf, f.i. enrolling interactive enquiries throughout an organization or mapping website visitors via a cloud application.	Notwithstanding the above, as reported in the EIOPA comments at Question 1, an undertaking has to ensure that it remains fully responsible for discharging all its obligations when outsourcing any function or activities (as stated in EIOPA System of Governance paragraph 1.14). For this reason, the Guidelines apply to any outsourcing to cloud service providers having their main focus on outsourcing of critical or important operational functions or activities. On the respondent request to eliminate the sentence "as a rule outsourcing should be assumed" from the Guideline, in order to align the Guidelines to the current practices in place for outsourcing, to make them more proportionate and in line to the approach chosen by the EBA in their outsourcing Guidelines, the presumption described above was removed, EIOPA deleted that sentence. **EIOPA updated the Guidelines accordingly**
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, there are insurers where Procurement & Outsourcing Policy covers the items of this Guideline, but not in all details (e.g. roles and responsibilities in detail, processes and reporting procedures etc.).	**EIOPA partially agrees with the concerns raised by the respondent.** As the Solvency II principles on outsourcing are still valid for cloud, with reference to the update of internal policies and procedures, multiple solutions are at disposal for undertakings: 1) development – where needed – of a dedicated cloud outsourcing policy; 2) complement - where needed – the undertaking outsourcing policy and the other relevant internal policies (for example the information security policy) to take into account the specificities of outsourcing to cloud service providers; and 3) if the undertaking current policies cover the elements described in these Guidelines, there is no need to update. In light of the above consideration, EIOPA updated the Guideline, enhancing its focus toward the outsourcing of critical or important functions or activities to cloud service providers. **EIOPA updated the Guidelines accordingly**
5b. Is the Guideline on written policy consistent to the market best practices on defining the policy for general outsourcing?	
Point 16f is not relevant for policy. It should be described per Material Outsourcing project/contract.	**EIOPA agrees with the concerns raised by the respondent and updated the Guidelines accordingly**

Response to the public consultation question	EIOPA Comments
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?	
Guideline 4 is too detailed and also captures information which is considers competitive. We advise to have a critical view of this and reconsider when is notification is required. Point 18a. The interconnections with other critical or important functions – what is the limit? Point 18h. Yes/No question or a detailed exit strategy?	**EIOPA agrees with the concerns raised by the respondent.** The content of Guideline 4 which is related only to outsourcing of critical or important operational functions or activities has been streamlined by: (a) removing the requirement to present a draft copy of the outsourcing agreement (b) aligning the requirements to the EBA requirements set by paragraph 54 of the EBA Guidelines on outsourcing to ensure market consistency for outsourcing to cloud service providers. On the point related to former paragraph 18(a), EIOPA removed the requirement to report to the supervisory authority the interconnections with other critical or important functions with the aim to align the content of the Guideline to the provisions set by EBA Guidelines on outsourcing. On the point related to former paragraph 18(h), which has been moved to paragraph 24(j) as part of the documentation requirements for critical or important operational functions or activities outsourced to cloud service providers, EIOPA confirms that it is a "Yes/No" question. **EIOPA updated the Guidelines accordingly**
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?	
The introduction of a register would have a significant impact, as information is stored in various sources (contract register, risk register etc.). Further, the register should be for material outsourcing only and not for non-material outsourcing (point 22).	**EIOPA partially agrees with the concerns raised by the respondent.** EIOPA has streamlined the content of the Guideline 5 in order to make it more principle and risk based by removing the requirements for keeping a register and requiring the undertaking to record information of their cloud outsourcing arrangements. Furthermore, EIOPA has defined, as minimum requirement, a set information to be recorded only for critical or important operational functions outsourced to cloud service providers. This set of information is aligned to the one required by the EBA Guidelines on Outsourcing. For outsourcing to cloud service providers on non-critical non-important operational functions or activities, the level of detail of the information to be recorded should be determined by the undertakings on a risk-based approach. **EIOPA updated the Guidelines accordingly.**
7b. What can be other approaches to ensure a proper and sound holistic oversight of cloud outsourcing?	

Response to the public consultation question	EIOPA Comments
Another approach would be a contract register containing meta data and separate enterprise risk management system that covers risks and architecture mapping and seca tool.	**EIOPA noted the concerns of the respondent.** EIOPA will take the suggestion into account in the process of reviewing the System of Governance Guidelines when a broader and comprehensive discussion on how document the outsourcing arrangements will be undertaken. **No changes were made to the Guidelines.**
8. Are the documentation requirements appropriate and sufficiently clear?	
- Point 23 b: the risk assessment summary is not included in register. The document is stored, risks are captured in iRisk -> enterprise risk mgt system. - Point 23g: time criticality is not adding value. Confidentiality, Integrity and Availability (CIA) rating will do. - Point 23h: BCP is a requirement, so it should always be yes. - Point 23i: is not feasible: only the name of contract owner and contract manager are stored centrally - We would like to add a validity date of relevant certificates held by the cloud service providers, their scope and the organization granting the certificate.	**EIOPA partially agrees with the concerns raised by the respondent.** In particular EIOPA: - kept the requirement to record the information at former paragraph 23(b), however, as reported above (Question 7a), an undertaking is free to define the best way to record such information; - - agrees with the respondent and removed the requirement to include the BCP as part of the set of minimum information to be recorded because the answer would have been always yes; - deleted the provision at former paragraph 23(i); - On the point related to the validity date of relevant certificates, while agreeing in principle with the respondent, EIOPA decided not to include the point in the documentation requirements. The suggestion into account in the process of reviewing the System of Governance Guidelines when a broader and comprehensive discussion on how document the outsourcing arrangements will be undertaken **EIOPA updated the Guidelines accordingly.**
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?	
Point 25: This wording is inconsistent with the text of article 274(5) of the Delegated Regulation, which reads "is outsourcing critical or important operational functions or activities.' The additions 'is related to' expands the scope compared to the Delegated Regulation. "Materially affecting the risk profile of the undertaking' is not in the Delegated Regulation either. We advise to delete it in order to make it consistent with the Delegated Regulation. We propose to integrate Guideline 4 and 7 and clarify which part of the Guidelines apply to outsourcing in general and which part to Material outsourcing only?	**EIOPA partially agrees with the concerns raised by the respondent.** On the use of the term "material" instead of the term "critical or important", as reported above, bearing in mind that one of the main purposes of these Guidelines is to provide clarity to the market participants, EIOPA decided to withdraw the use of the term "material outsourcing" sticking to the term "critical or important operational function and activity". On the proposal to merge Guideline 4 and 7, EIOPA has decided not to merge these Guidelines as EIOPA is the opinion that the current structure is deemed to be sufficiently clear.

Response to the public consultation question	EIOPA Comments
We can concur with this concept, but we notice that almost similar requirements are applicable to both material and non-material outsourcing contracts. We are of the opinion that non material outsourcing falls outside the scope.	On contractual requirements, EIOPA reviewed extensively the scope of application of Guideline 10 which will be applicable only in case of cloud outsourcing of critical or important operational functions or activities **EIOPA updated the Guidelines accordingly**
10. Is the content of Guideline on risk assessment of cloud outsourcing appropriate and sufficiently clear?	
Yes. EIOPA sees concentration risk at certain (large) cloud companies. We believe that it is not up to the (insurance) industry to mitigate this risk. From its nature, it takes high very high capital investments to offer cloud services; therefore a limited number of players is positioned to offer this kind of services. The matter of any concerns about this business being oligopoly is not to be solved by the industry.	**EIOPA noted the concerns raised by the respondent.** Knowing how much of an undertaking outsourcing is concentrated into one or more (cloud) service providers is a useful information that the decision making body should weigh in the risk assessment to decide whether or not outsource to that specific cloud service provider the specific service. The Guidelines do not preclude the outsourcing to cloud service providers with market dominance (or that is not easily substitutable) nor require the (re)insurance industry to substitute to the proper institutional body in charge to deal with the potential concerns regarding oligopoly in the cloud services industry. **No changes were made to the Guidelines.**
11. Are the contractual requirements for material outsourcing appropriate and sufficiently clear?	
Point 37: The extent the requirements go beyond the requirements in article 274 of the Solvency II Delegated Regulation, these should be included in the Solvency II Delegated Regulation and not included through a Guideline or mapped to the requirements in article 274. Not all requirements seem to be really 'additional' or are fairly obvious or not specific to cloud services so the question is if the additional requirements are necessary at all. Dealing with these requirements separately from the set of requirements in the Solvency II Delegated Regulation. Article 38 of the Solvency II Directive only applies of functions or insurance or reinsurance activity (i.e. only to material outsourcing). Point 38: This goes beyond what is required under the Solvency II Directive/Delegated Regulation.	**EIOPA partially agrees with the concerns raised by the respondent.** As reported above (at EIOPA comments to Question 9) EIOPA reviewed extensively the text of the Guideline 10 to ensure a better inclusion of the principle of proportionality. In light of this, EIOPA: (1) reviewed the scope of application of the Guideline which will be applicable only in case of cloud outsourcing of critical or important operational functions or activities; (2) clarified the relationship between this Guideline and the requirements set by Directive 2009/138/EC and Commission Delegated Regulation (EU) No 2015/35 by eliminating the former paragraphs 36 and 38. **EIOPA updated the Guidelines accordingly**
12. Are the criteria provided to set the contractual requirements for non-material outsourcing appropriate and sufficiently clear?	
No. Point 37 "…regardless of the materiality…. the outsourcing agreement should include all the requirements set out in Article 38 of the Solvency II Directive.", only describes right-to-audit, no further requirements. There does not seem to be a basis for setting contractual requirements for non-material outsourcing.	**EIOPA noted the concerns raised by the respondent.** As reported above (Question 11), reviewed the scope of application of the Guideline which will be applicable only in case of cloud outsourcing of critical or important operational functions or activities. As result the former paragraph 37 has been deleted.

Response to the public consultation question	EIOPA Comments
13. Are the Guideline on access and audit rights appropriate and sufficiently clear	
It remains somewhat unclear what exactly is expected of the industry on these points. Clarification what is expected in relation to the entire chain on this point would be helpful. On point 46 it is not clear what is expected from financial institutions on top of 3rd party assurance reports and certification. Cloud Service Providers may not easily give Right-to-audit. We would focus on the Scope of their certifications and present use cases on which you want assurance.	**EIOPA partially agrees with the concerns raised by the respondent.** As reported in paragraph 44 of the Guidelines (former paragraph 46), in case of outsourcing of critical or important operational functions to cloud service providers, undertakings should not rely solely on third-party certifications and reports as referred to in paragraph 42(a) over time. This means that undertakings do not simply assume that receiving a certificate or report is enough assurance that the cloud service is being provided in accordance with the legal, regulatory and risk management requirements set by the undertaking. If an undertaking elects to use third party certifications as audit tool, such undertaking should assess the adequacy of the information in these certifications against its own requirements and make follow-up enquiries to the cloud service providers if necessary (which might include the performance of on-site audits). When defining the scope of audits on its cloud outsourcing arrangements an undertaking should include an assessment of the service provider's and, where applicable, its significant sub-outsourcers' security and control environment, incident management process (in particular in case of data breaches, service disruptions or other material issues) and the undertaking's observance of these Guidelines in relation to cloud outsourcing arrangements. **EIOPA updated the Guidelines accordingly.**
14. Are the provisions set by this Guideline for security of data and systems appropriate and sufficiently clear?	
YES	NA
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, EIOPA requires a draft version of the contract. The Dutch regulator DNB requires a signed version. Would appreciate more guidance on proposed moment for notification, as we would like to understand this in relation to implementation process. It depends on the "material" size of the service, but we would opt for basic template with checklist. We would like to suggest that the Cloud Provider, provides this in a structured format (e.g. XML/JSON, etc.) for easy importing in various CMDBs.	**EIOPA noted the concerns raised by the respondent** Notwithstanding the fact that in the Netherlands and in other European Member States it is required by the national supervisory authority to present a copy of the outsourcing contractual arrangement as part of the notification package, on the basis of the feedback to the public consultation, EIOPA decided to remove that provision from the Guidelines. This decision was taken to align the content of the Guidelines to the EBA Guidelines on outsourcing and under the assumption that a broader and comprehensive discussion on how document the outsourcing arrangements will be undertaken when reviewing the System of Governance Guidelines.

Response to the public consultation question	EIOPA Comments
16. Do you have any comments on the impact assessment?	
Yes. We would prefer to have option 2.2 development of more detailed Guidelines on outsourcing arrangements as a whole instead of 2.1 dedicated cloud outsourcing Guidelines.	**EIOPA noted the concerns raised by the respondent** As reported in the impact assessment, EIOPA has chosen the policy option to develop cloud outsourcing Guidelines to timely, answer the increasing market practices of outsourcing to cloud service providers. However, taking into account the feedback to the Public consultation, in the process of reviewing the System of Governance Guideline, EIOPA will evaluate the option to merge these Guidelines with the updated version of the Guidelines on outsourcing.
Annex Y/N	
NO	

Association of Mutual Insurers and Insurance Cooperatives in Europe (AMICE), Belgium

Response to the public consultation question	EIOPA Comments
1. Is the scope of application provided appropriate and sufficiently clear?	
YES	NA
2. Is the set of definitions provided appropriate and sufficiently clear?	
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 above-mentioned 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.).	**EIOPA partially agrees with the concerns raised by the respondent.** Cloud service provider, EIOPA changed the definition by deleting the reference highlighted by the respondent. The point related to "third parties which are not cloud service providers but rely significantly on cloud infrastructure to provide their services" has been transferred in Guideline 1. The definition has been changed. Cloud broker, as the concept of cloud broker is not used in the Guidelines, EIOPA decided to delete the definition. The definition has been deleted. On the point related to technological neutrality, EIOPA removed the reference to the cloud service models (SaaS, IaaS and PaaS) and the related definitions along the Guidelines and replaced this text with a more generic reference to 'cloud service models'. **EIOPA updated the Guidelines accordingly.**
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?	
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	**EIOPA partially agrees with the concerns raised by the respondent.** EIOPA moved the date of application to 1 January 2021 and prolonged the period for reviewing the existing arrangements to 31 December 2022. Moreover, in order to make the Guidelines more proportionate, a principle of risk-based review has been introduced (i.e. only contract related to critical and important operational functions should be amended). Furthermore, the flexibility clause contained in the draft version of the Guidelines (former paragraph 9, current paragraph 12) has been kept. **EIOPA updated the Guidelines accordingly.**

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?	
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.	**EIOPA partially agrees with the concerns raised by the respondent.** The determination of whether (or not) the purchase of cloud services fall into the scope of outsourcing is paramount to a successful and coherent application of these Guidelines. To perform this determination is responsibility of the undertakings and should be carried out by applying the criteria provided in Guideline 1 and in the regulatory obligations listed in the introduction of these Guidelines. There are two type of arrangements with third parties service providers: 1) Services which are not outsourcing (for example, non-recurrent activities and purchases of goods – including software licences – are not considered as outsourcing arrangements) and 2) Services, which are outsourcing. Among the services which are outsourcing there is a distinction between: (i) outsourcing of critical or important operational functions (which includes, but is not limited to, insurance and reinsurance processes and activities, functions as defined by Solvency II art. 13(29), provisioning of on-going day to day systems maintenance or support, investment of assets or portfolio management, etc.) (ii) outsourcing of non-critical, non-important operational functions (i.e. less material). In case of outsourcing, an undertaking has to ensure that it remains fully responsible for discharging all its obligations when outsourcing any function or activities (as stated in EIOPA System of Governance paragraph 1.14). For the outsourcing of critical or important operational functions or activities, an undertaking must meet certain requirements. When an undertaking purchases cloud services, it has to perform the same type of assessment due in case of "general outsourcing", namely 1) understand whether the purchase of cloud services is outsourcing or not; 2) if it classifies as outsourcing, understand whether the outsourced function is critical or important; 3) on critical or important operational functions or activities, perform a detailed risk assessment on the operational function/activity to be outsourced and a detailed due diligence on the service provider;

	4) On all the less material outsourcing, in order to fulfil its responsibility obligation (as stated above), a risk assessment and a due diligence (of higher level compared to the previous point) are to be performed. Furthermore, notwithstanding the results of the assessment of whether or not the provisioning of cloud services falls under the definition of "outsourcing", as part of their internal control system, on a risk and proportionate way, the undertaking should identify, measure, monitor, manage and report risks caused by arrangements with third parties regardless whether or not those third parties are cloud service providers. EIOPA agrees with the respondent on the fact that, in principle, only on outsourcing, an undertaking should perform an assessment on whether the operational function or activity outsourced is a critical or important. For this reason, the Guidelines apply to any outsourcing to cloud service providers having their main focus on outsourcing of critical or important operational functions or activities. On the respondent request to eliminate the sentence "as a rule outsourcing should be assumed" from the Guideline, in order to align the Guidelines to the current practices in place for outsourcing, to make them more proportionate and in line to the approach chosen by the EBA in their outsourcing Guidelines, the presumption described above was removed, EIOPA deleted that sentence. **EIOPA updated the Guidelines accordingly**
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?	
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	**EIOPA agrees with the concerns raised by the respondent** On the timeline to update their outsourcing policies (where needed) the point on the Guideline has been clarified and set to 1 January 2021. On the point related to former paragraphs 16(d) and (f) (current paragraphs 20 (d) and (f)), EIOPA clarified in the text of the Guideline that they are applicable only to critical or important operational functions or activities. **EIOPA updated the Guidelines accordingly**

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 ?	
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.	**EIOPA agrees with the concerns raised by the respondent and updated the Guidelines accordingly**
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?	
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.	**EIOPA partially agrees with the concerns raised by the respondent.** The content of Guideline 4 which is related only to outsourcing of critical or important operational functions or activities has been streamlined by: (a) removing the requirement to present a draft copy of the outsourcing agreement (b) aligning the requirements to the EBA requirements set by paragraph 54 of the EBA Guidelines on outsourcing to ensure market consistency for outsourcing to cloud service providers. As a result of the exercise of harmonisation with the requirements of the EBA Guidelines on outsourcing, The former paragraph 18(d) has been removed from the Guidelines. **EIOPA updated the Guidelines accordingly.**
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	**EIOPA noted the concerns raised by the respondent.**
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. In relation to question 7a, 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.	**EIOPA partially agrees with the concerns raised by the respondent.** EIOPA has streamlined the content of the Guideline 5 in order to make it more principle and risk based by removing the requirements for keeping a register and requiring the undertaking to record information of their cloud outsourcing arrangements. Furthermore, EIOPA has defined, as minimum requirement, a set information to be recorded only for critical or important operational functions outsourced to cloud service providers. This set of information is aligned to the one required by the EBA Guidelines on Outsourcing. For outsourcing to cloud service providers of non-critical non-important operational functions or activities, the level of detail of the information to be recorded should be determined by the undertakings on a risk-based approach. EIOPA will undertake a broader and comprehensive discussion on how to document discussion on how document outsourcing arrangements when reviewing the System of Governance Guideline. **EIOPA updated the Guidelines accordingly.**
8. Are the documentation requirements appropriate and sufficiently clear?	
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).	**EIOPA agrees with the concerns raised by the respondent.** As reported above EIOPA has defined, as minimum requirement, a set information to be recorded only for critical or important operational functions outsourced to cloud service providers. On the point related to former paragraph 23(i), EIOPA agrees with the respondent and decided to remove it from the list of information to be registered. **EIOPA updated the Guidelines accordingly.**
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?	
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.	**EIOPA partially agrees with the concerns raised by the respondent.** On the use of the term "material" instead of the term "critical or important", as reported above, bearing in mind that one of the main purposes of these Guidelines is to provide clarity to the market participants, EIOPA decided to

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.	withdraw the use of the term "material outsourcing" sticking to the term "critical or important operational function and activity". **EIOPA updated the Guidelines accordingly.**
10. Is the content of Guideline on risk assessment of cloud outsourcing appropriate and sufficiently clear?	
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.	**EIOPA partially agrees with the concerns raised by the respondent.** On the request to remove the wording "both before and after the outsourcing" at Guideline 8, EIOPA clarified in the Guideline when a review of the risk assessment should be performed. On the cost-benefit analysis, the provision has been clarified in order to make it more proportionate. The provisions at former paragraphs 30(a) to (h) (currently reported in paragraph 31(b)) have been reviewed and streamlined. On the point related to the review of the risk assessment, EIOPA agrees with the concerns raised by AMICE and, as reported above, decided to review the former paragraph 31 (current paragraph 32), which now clarifies when a review of the risk assessment should be performed. **EIOPA updated the Guidelines accordingly.**
11. Are the contractual requirements for material outsourcing appropriate and sufficiently clear?	
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.	**EIOPA partially agrees with the concerns raised by the respondent.** On Guideline 10 (contractual requirements)

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).	EIOPA acknowledges that negotiating non-standard contractual clauses with cloud service providers could be challenging in particular for smaller undertakings. For this reason and bearing in mind the possible complexities of its implementation in case of misalignments between the content of this Guideline and of the one set by the EBA on the same subject, EIOPA further aligned the wording of this Guideline to the EBA requirements set by paragraph 75 of the EBA Guidelines on outsourcing. Furthermore, EIOPA clarified the relationship between this Guideline and the requirements set by Directive 2009/138/EC and Commission Delegated Regulation (EU) No 2015/35. On the specific requests to amend elements of the Guidelines, EIOPA: - EIOPA kept the same wording as defined by the EBA Guidelines on data localisation (former paragraph 35 (g), currently 37(f)) and on access and audit rights (current paragraph 35(m), aligned to paragraph 87 of the EBA Guidelines); - On the request to delete former paragraph 35 (m), EIOPA kept the requirement. The expression "written agreement" is the same used in the Guidelines on System of Governance and therefore it has been kept. EIOPA is aware that there might be more documents to describe the business relationship between an undertaking and its cloud service providers and that the contents of the Guideline 10 can be included in one or more of them. On the possibility to organise a workshop with cloud service providers on these Guidelines, EIOPA will evaluate this possibility in 2020. <u>On Guideline 9 (due diligence)</u> EIOPA agrees with the concerns raised by AMICE. For this reason, to ensure a better inclusion of the principle of proportionality, EIOPA reviewed the content of the Guideline 9. Particularly, EIOPA: (1) included a specific paragraph in the Guideline to specify that if an undertaking enters into a second agreement with a cloud service provider already assessed by that undertaking, the undertaking should determine, on a risk-based approach, whether a second due diligence is needed; (2) better distinguished between the due diligence to be performed on cloud service providers in case a critical or important operational

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".	function or activity is outsourced to them *versus* the due diligence on cloud service providers for less material outsourcing. In order to evaluate the suitability of the cloud service provider, an undertaking could use certificates based on international standards. These include but are not necessarily limited to International Safety Information Security Standard ISO / IEC 2700X of the International Organization for Standardization, C 5 Requirement Catalogue of the Federal Office for Information Security, Cloud Security Alliance standards. **EIOPA updated the Guidelines accordingly.**
12. Are the criteria provided to set the contractual requirements for non-material outsourcing appropriate and sufficiently clear?	
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.	**EIOPA agrees with the concerns raised by the respondent and updated the Guidelines accordingly.**
13. Are the Guideline on access and audit rights appropriate and sufficiently clear	
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	**EIOPA disagrees with the concerns raised by the respondent.** In order to foster the development of European-wide standards in the area of auditing cloud services for financial institutions, EIOPA aligned the conditions to use third party certifications or audit reports to the ones set by the EBA Guidelines on outsourcing (paragraphs 92-93). These conditions include, in case of outsourcing of critical or important operational functions or activities to cloud service providers, the requirement for the undertakings to not rely solely on third-party certifications and reports over time. This means that undertakings should not simply assume that receiving a certificate or a report is enough assurance that the cloud service is being provided in accordance with their legal, regulatory and risk management obligations. If an undertaking elects to use third party certifications as audit tool, such undertaking should assess the adequacy of the information in these certifications against its own requirements and make follow-up enquiries to the cloud service providers if necessary (which might include the performance of on-site audits).

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?	
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.	**EIOPA agrees with the concerns raised by the respondent.** EIOPA clarified that the main scope of the Guideline 12 (i.e. paragraphs 48 and 49) are critical or important operational functions outsourced to cloud service providers. On the point related to outsourcing the activities foreseen by the Guideline, being not different from other activities performed by them, undertakings can outsource these activities to third parties**.** Such outsourcing will be subject to the Solvency II provisions on outsourcing and for this reason that possibility has not been mentioned in the Guidelines. **EIOPA updated the Guidelines accordingly.**
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.	
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.	**EIOPA partially agrees with the concerns raised by the respondent.** Acknowledging that the scope of these Guidelines (i.e. outsourcing to cloud service providers) is narrower than the one of EBA Guidelines on outsourcing and aiming at embedding the principle of proportionality and a risk-based approach on their implementation, EIOPA streamlined the contents of the Guidelines, mainly focusing on outsourcing of critical or important operational functions or activities to cloud service providers. These changes have been done to emphasize EIOPA willingness to focus on substance over form. On the provision contained at former paragraph 58 in relation to the concentration risk, EIOPA agrees with the respondent and removed the provision from the Guidelines. As well EIOPA clarified that the AMSB should be periodically updated on the risks identified in respect of its cloud outsourcing of critical or important operational functions or activities. Such update, for instance, could be performed as part of the periodical updates to the AMSB on the operational resilience of the undertaking or on the performances of the outsourcers. **EIOPA updated the Guidelines accordingly.**

16. Do you have any comments on the impact assessment?	
No comment	NA
Annex Y/N	
YES	

German Insurance Association (GDV e.V.), Germany

Response to the public consultation question	EIOPA Comments
1. Is the scope of application provided appropriate and sufficiently clear?	
General comments: We welcome EIOPA's aims to provide clarification and transparency to market participants avoiding potential regulatory arbitrage as well as to foster supervisory convergence. However, in our view the Guidelines should remain limited to what is really necessary and helpful. The usage of cloud services is in principle not different from requesting any other service from third parties or a group entity. If the accumulation of cloud services qualifies for outsourcing, regulatory requirements set out Articles 49 Paragraphs 2 and 3 Directive 2009/138/EG and 274 Paragraphs 2 to 5 in Commission Delegated Regulation apply; EIOPA should refrain from establishing an exclusive outsourcing regime for cloud computing. However, the extensive scope of the Guidelines generates redundancies to existing rules and to the EIOPA Guidelines on the System of Governance in particular. In addition, the introduction of new terms like "material outsourcing" not only creates the impression that EIOPA generally attributes an increased regulatory risk to cloud outsourcing; some Guidelines impose even stricter requirements than for outsourcing of critical or important operational functions. EIOPA should not introduce a terminology that is not in line with the level 1 and level 2 texts (which provide for "outsourcing of critical and important functions and services"). Therefore, the GDV would urge EIOPA to revisit its approach and instead just focus on the "translation" of existing requirements to a limited number of special aspects and issues related to cloud computing. Otherwise, the compliance with the regulatory expectations set out in the Guidelines could disincentive insurers from using cloud technology with detrimental effects on their global competitiveness. This would contrast the public commitment of the EU Commission to elevate the European Union to a leading place for digital technology. In this context we also suggest considering direct supervision of cloud-provider instead of further industry-specific requirements. Both the headline and the introduction (in particular Paragraph 1) imply that claiming cloud services always constitute an outsourcing arrangement. However, cloud services not related to typical insurance business activities are not subject to prudential outsourcing provisions. The language of the draft Guidelines should take account of this more clearly. Lastly it remains unclear	**EIOPA noted the concerns raised by the respondent.** Please, see the EIOPA comments to the concerns raised by the respondent at the section dedicated to EIOPA comments for each single question.

Response to the public consultation question	EIOPA Comments
whether the requirements for non-insurance entities in a group should be implemented.	
2. Is the set of definitions provided appropriate and sufficiently clear?	
Art. 13 No. 29 of Directive 2009/138/EG defines a "function" as special tasks embedded in the system of Governance. Paragraph 6 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. 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 pursuant to Article 274 Paragraph 3 of the Delegated Regulation. 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 cloud service provider. The definition of "cloud brokers" is dispensable as they are not addressed in the draft Guidelines.	**EIOPA partially agrees with the concerns raised by the respondent.** Function, in order to avoid the possible confusion with Article 13(29) of Solvency II Directive, EIOPA decided to delete the definition. The definition has been deleted On the definition of Material outsourcing, on the basis of the feedback received and bearing in mind that one of the main purposes of these Guidelines is to provide clarity to the market participants, EIOPA decided to withdraw the use of the term "material outsourcing" sticking to the term "critical or important operational function and activity". The definition has been deleted Cloud service provider, EIOPA changed the definition by deleting the reference highlighted by the respondent. The point related to "third parties which are not cloud service providers but rely significantly on cloud infrastructure to provide their services" has been transferred in Guideline 1. The definition has been changed. Cloud broker, as the concept of cloud broker is not used in the Guidelines, EIOPA decided to delete the definition. The definition has been deleted. **EIOPA updated the Guidelines accordingly.**
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?	
Implementation of the Guidelines would require a complex restructuring of existing cloud arrangements and their migration into the register. The restructuring of existing cloud arrangements may also have legal ramifications as the Guidelines would interfere in contractual relationships subject to Civil Law. Any modifications of existing arrangements require the cooperation and agreement of the cloud service providers. This can be a lengthy renegotiation process and the duration and success of this is not in the hands of insurance companies alone. Given this background, the implementation process would be very costly and hardly enforceable until 1 July 2022, but likely to end up in a continuous effort. Therefore, we request EIOPA to grant a grandfathering of all cloud arrangements concluded until 1 July 2020.	**EIOPA partially agrees with the concerns raised by the respondent.** EIOPA moved the date of application to 1 January 2021 and prolonged the period for reviewing the existing arrangements to 31 December 2022. Furthermore, clarification on the due date to perform the update (where needed) to the undertaking policies and internal processes in accordance to the Guidelines has been clarified and set to 1 January 2021. On the proposal to grandfather the existing obligation, EIOPA has not agreed with the proposal. However, in order to make the Guidelines more proportionate, a principle of risk-based review has been introduced (i.e. only contract related to critical and important operational functions should be amended). Furthermore, the flexibility clause contained in the draft version of the Guidelines (current paragraph 12) has been kept. **EIOPA updated the Guidelines accordingly**

Response to the public consultation question	EIOPA Comments
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?	
By assuming outsourcing as a rule, the assessment process described in Paragraph 10 would be virtually obsolete. Moreover, it is questionable from a legal view to work with assumptions and allocate the burden to proof the contrary to the supervised undertakings. It should be sufficient to sensitize supervisors and undertakings that cloud transactions may have to comply with outsourcing provisions without predetermining the outcome. Paragraph 12 should be deleted as the activities performed as part of the internal control system are not particularly related to cloud services. Any such general statements should be integrated in the Guidelines on the System of Governance where the subject-matter is treated by EIOPA.	**EIOPA partially agrees with the concerns raised by the respondent** The determination of whether (or not) the purchase of cloud services fall into the scope of outsourcing is paramount to a successful and coherent application of these Guidelines. To perform this determination is responsibility of the undertakings and should be carried out by applying the criteria provided in Guideline 1 and in the regulatory obligations listed in the introduction of these Guidelines. On the point of former paragraph 12, EIOPA agrees with the concerns raised by the GDV and removed the provision from the Guidelines. As suggested by the respondent, EIOPA will take the content of the former paragraph 12 into account in the process of reviewing the System of Governance Guidelines. **EIOPA updated the Guidelines accordingly**
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?	
We reiterate the concern already stated in our general comments: The Guidelines should focus on particular aspects characteristic of cloud computing which require a translation or interpretation of existing requirements. However, 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 also may create the inadequate impression that existing requirements could be applied in a different way when it comes to cloud outsourcing. The term "IT function" used in paragraph 16 lit. a. is misleading as it is not a defined key function. We suggest clarification by using a different terminology, e.g. "IT division". Apart from that, Paragraph 16 lit. f. requires undertakings to document a termination strategy for outsourcing arrangements regardless their materiality. This is disproportionate for non-material outsourcing transactions. The underlying functions or activities are not essential for the continuity of obligations and services to the policyholders. In general, the GDV would also question EIOPA's 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 "regular" outsourcing arrangements. Therefore, the written policy according to Article 274 Paragraph	**EIOPA partially agrees with the concerns raised by the respondent** As the Solvency II principles on outsourcing are still valid for cloud, with reference to the update of internal policies and procedures, if the undertaking current policies cover the elements described in these Guidelines, there is no need to perform any update to them. In light of the above consideration, EIOPA updated the Guideline, enhancing its focus toward the outsourcing of critical or important functions or activities to cloud service providers. - On the point on former paragraph 16(f) (currently paragraph 20(f)) related to the 'exit strategy', EIOPA agrees with the by the respondent and updated the Guideline accordingly. On the role of the AMSB as set by Guideline 2, EIOPA agrees with the by the respondent and updated the Guideline accordingly. **EIOPA updated the Guidelines accordingly**

Response to the public consultation question	EIOPA Comments
1 of the Delegated Regulation has to be also (and comprehensively) applicable to outsourcings to the cloud. With regard to Guideline 2, the GDV 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 Paragraph 3 of the Delegated Regulation, the AMSB only needs to establish a process which ensures compliance with the requirements on the outsourcing of critical or important functions and to confirm the general terms of the outsourcing agreement.	
5b. Is the Guideline on written policy consistent to the market best practices on defining the policy for general outsourcing ?	
With reference to the consistency with market best practices, the GDV would like to point out that it should be left to the discretion of the supervised undertakings how to integrate cloud issues in their overall outsourcing policy. There is no legal requirement that stipulates a separate treatment.	**EIOPA agrees with the concerns raised by the respondent.** Insurance undertakings have at their disposal multiple solution to transpose these Guidelines into their internal policies and procedures: - development – where needed – of a dedicated cloud outsourcing policy; - complement - where needed – the undertaking outsourcing policy and the other relevant internal policies (for example the information security policy) to take into account the specificities of outsourcing to cloud service providers; and - if the undertaking current policies cover the elements described in these Guidelines, there is no need to update. **EIOPA updated the Guidelines accordingly**
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?	
The requested information according to Guideline 4 is due to the obligation to submit the contract in draft partially redundant, widely exceeds Level 1-requirements and goes way beyond of what is deemed necessary by EIOPA itself with regard to the notification of "regular" outsourcing transactions. Article 49 Paragraph 3 of Directive 2009/138/EG does not specify the content of the notification. EIOPA-Guideline 64 on system of governance solely requires a description of the scope and the rationale for the outsourcing and the service provider's name. There is no legal argument or a supervisory rationale to demand, for instance, an assessment on the cloud service provider's substitutability.	**EIOPA partially agrees with the concerns raised by the respondent** The content of Guideline 4 which is related only to outsourcing of critical or important operational functions or activities has been streamlined by: (a) removing the requirement to present a draft copy of the outsourcing agreement (b) aligning the requirements to the EBA requirements set by paragraph 54 of the EBA Guidelines on outsourcing to ensure market consistency for outsourcing to cloud service providers. **EIOPA updated the Guidelines accordingly**
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?	

Response to the public consultation question	EIOPA Comments
Yes. Irrespective of the lack of legal means for competent authorities to require such a register, its establishment and maintenance would be very time consuming and costly. These costs are not justified by a meaningful supervisory purpose as the competent authorities are fully aware of the magnitude of cloud outsourcing arrangements due to the notification by the insurers. In addition, competent authorities are not prevented to request further information, if necessary. Therefore, we propose that extensive documentation should only be necessary upon request of the national supervisor. It should be up to the supervised undertakings how to ensure that such information requests can be complied with and information on all cloud arrangements is readily available. Additionally the centralised, group-wide management of such contracts should not be regarded as the rule (Paragraph 21). According to our understanding of the principle-based approach, a group does not necessarily need a unique group-wide database. According to the general requirements of risk management, it may be sufficient if effective management is guaranteed. Due to company law freedoms, it is rather the practice that different IT environments are quite common for large groups. It is desirable that a pragmatic solution is found here that takes into account and adequately appreciates the current state of large groups.	**EIOPA partially agrees with the concerns raised by the respondent.** EIOPA has streamlined the content of the Guideline 5 in order to make it more principle and risk based by removing the requirements for keeping a register and requiring the undertaking to record information of their cloud outsourcing arrangements. Furthermore, EIOPA has defined, as minimum requirement, a set information to be recorded only for critical or important operational functions outsourced to cloud service providers. This set of information is aligned to the one required by the EBA Guidelines on Outsourcing. For outsourcing to cloud service providers on non-critical non-important operational functions or activities, the level of detail of the information to be recorded should be determined by the undertakings on a risk-based approach. The content of the former paragraph 21 on centralised management of the register of cloud outsourcing arrangements has been removed. The aim of EIOPA was to give the possibility to groups to leverage on their scale by keeping track of their cloud outsourcing arrangements centrally as facultative option. EIOPA acknowledges that the changes made are a major departure from the requirements set by EBA Guidelines on outsourcing, which requires firms to maintain a register on all outsourcing arrangements. This decision was taken under the assumption that a broader and comprehensive discussion on how document the outsourcing arrangements will be undertaken when reviewing the System of Governance Guidelines. **EIOPA updated the Guidelines accordingly**
7b. What can be other approaches to ensure a proper and sound holistic oversight of cloud outsourcing?	
NO COMMENT	NA
8. Are the documentation requirements appropriate and sufficiently clear?	
The bulk of information is excessive and leads towards an alignment of the requirements for non-material and material outsourcing. Moreover, it remains unclear whether the register is related to outsourced functions (Paragraph 19) or the cloud outsourcing arrangements (Paragraph 21). If EIOPA maintains its position on documentation requirements, the final Guidelines must clarify the scope. In this case, we suggest registering outsourcing arrangements only. Paragraph 22 effectively pretends a notification requirement for non-material outsourcing arrangements. This would undermine Level 1- restrictions.	**EIOPA partially agrees with the concerns raised by the respondent.** In particular, EIOPA clarified that the register should be kept for cloud outsourcing arrangements related to critical or important operational functions or activities. As reported above, the content of former paragraph 22 has been reviewed in order to avoid an unwanted notification before outsource to cloud service providers non-critical non-important operational functions or activities.

Response to the public consultation question	EIOPA Comments
	EIOPA updated the Guidelines accordingly.
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?	
We do not see the need to introduce new terms or concepts next to the outsourcing of critical or important operational functions. And we do not agree to requirements on the materiality assessment which would even exceed the requirements on outsourcing critical or important operational functions (Article 274 Paragraph 3 of the Delegated Regulation): Guideline 6 (Paragraph 24 lit. c. and d.) transfers 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. Moreover, there is no legal reference for requiring to calculate a cost ratio of cloud expenses to total operational and ICT costs (Paragraph 27 lit.e.): The same is true for substitutability assessments of cloud service providers (Paragraph 27 lt. 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. After all, there is no regulation deficit with regard to outsourcing in general and cloud outsourcing in particular. Additionally the large number of requirements to evaluate - and document - when assessing materiality of cloud outsourcing seems to be impracticable. As already mentioned we see no reason to treat cloud outsourcing other than "normal" outsourcing.	**EIOPA partially agrees with the concerns raised by the respondent.** On the use of the term "material" instead of the term "critical or important", as reported above, bearing in mind that one of the main purposes of these Guidelines is to provide clarity to the market participants, EIOPA decided to withdraw the use of the term "material outsourcing" sticking to the term "critical or important operational function and activity". On the comments related to Guideline 6: - in paragraph 27(c) (former paragraphs 24(c)), EIOPA clarified the provision making reference to Guideline 9 where a clear differentiation has been made between the type of due diligence requested in case of outsourcing to critical or important operational functions or activities *versus* in case of less-material outsourcing; - EIOPA did not change in paragraph 27(d) (former paragraph 24(d)), as it considers that an assessment of conflict of interests should be performed in line to the requirement – for the undertaking – to be fully responsible for discharging all its obligations when outsourcing any function or activities (as stated in EIOPA system of governance paragraph 1.14); On the comment related to former paragraph 27(a) vi, agreed with the suggestion of the respondent and removed the point. Being aim of these Guidelines to (a) provide clarification and transparency to market participants avoiding potential regulatory arbitrages; and (b) foster supervisory convergence regarding the expectations and processes applicable in relation to cloud outsourcing, EIOPA is the opinion that the criteria provided in to assess whether or not an operational function or activity outsourced to cloud service providers are not contradicting the requirements on outsourcing. **EIOPA updated the Guidelines accordingly.**
10. Is the content of Guideline on risk assessment of cloud outsourcing appropriate and sufficiently clear?	
The exhaustive level of detail of Guideline 8 reveals a general problem of EIOPA's approach. The distinction between the materiality assessment according to Guideline 7 and the risk assessment is blurred. There are a number of redundancies in terms of aspects to be considered. These redundancies arise from their separate treatment in different Guidelines. In contrast, we believe that the materiality assessment is an indispensable and	**EIOPA partially agrees with the concerns raised by the respondent.** EIOPA reviewed extensively the content of this Guideline to ensure a better inclusion of the principle of proportionality by: (1) reducing the number of areas to be checked during the risk assessment; (2) enhancing the flexibility of application of the Guideline; (3) focusing the scope of application of the

Response to the public consultation question	EIOPA Comments
integral part of the risk assessment and part of the qualification of any outsourcing. However, this question does not relate to cloud computing in particular and should be addressed, if considered necessary, in a wider context to general outsourcing transactions. Apart from that, some content of Guideline 8 is partly not required under Level 1-regulation: - Scenario analysis for strategic risk (Paragraph 28); - AMSB-approved cost-benefit analysis (Paragraph 29), - With regards to paragraph 30 lt. I it might not be easy for a single insurance company to define which cloud-provider is a dominant one. - 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 that cloud services are highly standardized. It is also stated that the risk assessment should be updated on a periodical basis. The GDV believes that an update is only warranted if the legal or contractual circumstances have changed.	Guideline only on critical or important operational functions and activities outsourced. On the specific requests to amend elements of the Guidelines, EIOPA: - deleted former paragraph 28; - deleted the provision related to an AMSB-approved cost-benefit analysis; - wishes to specify that having an understanding on whether the cloud service provider has a market dominance or that it is not easily substitutable could be a useful information that the decision making body should weigh in the risk assessment to decide whether or not outsource to that specific cloud service provider the specific service. The Guidelines do not preclude the outsourcing to cloud service providers with market dominance or that it is not easily substitutable; - clarified in the Guideline when a review of the risk assessment should be performed. **EIOPA updated the Guidelines accordingly.**
11. Are the contractual requirements for material outsourcing appropriate and sufficiently clear?	
Article 274 Paragraph 4 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 ("in addition to the set of requirements defined by Article 274…"). We would question EIOPA's authority to do so and see no benefit in the additional requirements. 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 lit. l. implies that this issue has to be addressed in the insurance contract. 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" (Paragraph 36). Article 274 does not attribute special emphasis on single requirements set out in Paragraph 4). Guideline 9 requires undertakings to conduct a due diligence assessment on the cloud service provider. On the one hand the requirements are too extensive and on the other hand there is no legal foundation for such a requirement. In particular, the requirement can't be justified with the reference to the obligation to perform a detailed examination to ensure that the potential	**EIOPA partially agrees with the concerns raised by the respondent.** On Guideline 10 (contractual requirements) EIOPA reviewed extensively the text of the Guideline to ensure a better inclusion of the principle of proportionality. In light of this, EIOPA: (3) reviewed the scope of application of the Guideline which will be applicable only in case of cloud outsourcing of critical or important operational functions or activities; (4) clarified the relationship between this Guideline and the requirements set by Directive 2009/138/EC and Commission Delegated Regulation (EU) No 2015/35 by eliminating the former paragraphs 36, 37 and 38. Furthermore, bearing in mind the possible complexities of its implementation in case of misalignments between the content of this Guideline and of the one set by the EBA on the same subject, EIOPA further aligned the wording of this Guideline to the EBA requirements set by paragraph 75 of the EBA Guidelines on outsourcing.

Response to the public consultation question	EIOPA Comments
service provider has the ability, the capacity and any authorisation required by law to deliver the required functions or activities satisfactorily (Article 274 Paragraph 3 lit. (a) of the Delegated Regulation). This examination is not the same as a due diligence assessment as the legislator's reference in Article 256 Paragraph 2 of the Delegated Regulation confirms.	On Guideline 9 (due diligence) The legal basis of that requirement are the Article 49 of Solvency II Directive, the article 274 (3) of Solvency II Delegated Regulation and paragraph 1.14 of the System of Governance Guidelines. On the possible confusion between the term "due diligence" used in these Guidelines and the one used at Article 256 of Commission Delegated Regulation (EU) No 2015/35, EIOPA is the opinion that there is no confusion and therefore made no changes. **EIOPA updated the Guidelines accordingly.**
12. Are the criteria provided to set the contractual requirements for non-material outsourcing appropriate and sufficiently clear?	
Article 38 of Directive 2009/138/EG does not refer to contract requirements at all.	**EIOPA noted the concerns raised by the respondent.**
13. Are the Guideline on access and audit rights appropriate and sufficiently clear	
It is not entirely clear what the term „significant outsourcers'" is supposed to refer to in Paragraph 41. The GDV 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. Article 43 does not provide helpful guidance as the undertaking's audit requirements maintain even if their exercise would create a risk for the cloud service provider. There is little room for contractual agreements on alternative methods. 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 organizational resources of undertakings and cloud service providers. Even worse, Paragraph 46 prohibits undertakings to solely rely on these reports "over time", without specifying this period nor providing guidance to 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 lt. d). In addition, as long as it is not clear under which conditions insurers can rely on third-party reports or pooled audits, they have to do on-site visits themselves or need a representative at the pooled audits. Since cloud service providers charge their clients for on-site visits and audits, this leads to costs that might be affordable for large insurance companies.	**EIOPA partially agrees with the concerns raised by the respondent.** EIOPA clarified the scope of application of the Guideline, which will be applicable only in case of cloud outsourcing of critical or important operational functions or activities. Furthermore, in order to foster the development of European-wide standards in the area of auditing cloud services for financial institutions, EIOPA aligned the conditions to use third party certifications or audit reports to the ones set by the EBA Guidelines on outsourcing (paragraphs 92-93). These conditions include, in case of outsourcing of critical or important operational functions or activities to cloud service providers, the requirement for the undertakings to not rely solely on third-party certifications and reports over time. This means that undertakings should not simply assume that receiving a certificate or a report is enough assurance that the cloud service is being provided in accordance with their legal, regulatory and risk management obligations. If an undertaking elects to use third party certifications as audit tool, such undertaking should assess the adequacy of the information in these certifications against its own requirements and make follow-up enquiries to the cloud service providers if necessary (which might include the performance of on-site audits). **EIOPA updated the Guidelines accordingly.**

Response to the public consultation question	EIOPA Comments
However, it might refrain smaller insurance companies from using cloud services and thus limit competition among them. With regards to paragraph 45 lt. g the contractual right to expand the scope of certifications or controls for every single insurance company seems to be unrealistic. From our point of view it should be sufficient for the cloud provider having standardized 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. The contractual right to perform individual on-site inspections makes little sense as cloud service providers can hardly provide the resources to ensure a vast number of such inspections. Therefore, we welcome EIOPA's clarification in Paragraph 45 lit. h. that on-site inspections are not to be exercised on a regular basis but only in case of specific needs.	
14. Are the provisions set by this Guideline for security of data and systems appropriate and sufficiently clear?	
Paragraph 49 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. Moreover we suggest a different wording for Paragraph 50 lit. f. as it is somewhat misleading. The Paragraph could be misconstrued as requiring every company to enter into a comprehensive risk analysis of the data protection systems of all individual states with every service provider in advance, even if neither party intended to process data outside of the EU. While we doubt that EIOPA intends to introduce such extensive duties that would far surpass the requirements established by the GDPR and render the standard contractual clauses and adequacy decisions of the EU- Commission obsolete, adjustments to the wording would create more legal certainty. Paragraph 52 is likely to be extremely difficult to implement in practice. This is particularly the case where one or more subsidiaries have outsourced their IT to the parent company and the parent company uses a cloud service. Due to the already mentioned excessive definition of the term cloud service, the cloud service provider of the parent company would be a sub-service provider from the point of view of the subsidiary. All intra-group outsourcing agreements would require adjustment. In addition, the requirements would probably be even more difficult to implement in practice if the cloud service provider of the parent company in turn provided significant parts of the	**EIOPA partially agrees with the concerns raised by the respondent.** On Guideline 12 (Security of data and systems) EIOPA assessed the Guidelines before and after the consultation and did not identify this as an area that would contradict the GDPR. To avoid misunderstandings the word "on-going" has been substituted with the word "regular". On the specific requests to amend or clarify specific elements of the Guidelines: - EIOPA changed the word "ongoing" with the word "regular" at former paragraph 49 (now, paragraph 48) - EIOPA removed the reference to the definition of a data residency policy and substituted it with a more principle based instruction; On Guideline 13 (Sub-outsourcing of critical or important operational functions or activities) EIOPA removed the former paragraph 52, however wishes to clarify that in case of groups and intra-group outsourcing where cloud infrastructure is used directly or as part of the sub-outsourcing chain, such arrangements also fall within the scope of these Guidelines.

Response to the public consultation question	EIOPA Comments
relevant cloud services through other group companies or with the help of external third parties. Paragraph 55, in its current wording, provides from our point of view an inappropriate coexistence of rights: In the sense of legal certainty, a tiered relationship between objection and termination is desirable. For the same reason, Paragraph 60 should clarify when termination is necessary. The in Paragraph 56 established requirements for monitoring are very extensive. The GDPR does not require continuous monitoring (see also the comment to Paragraph 49 above). The requirement of complete and irrevocable deletion laid down in Paragraph 60 lit. d is not or hardly possible according to the current state of the art. Against the background of the unity of the legal system, it should suffice to safeguard the interests of the insured persons if the characteristics "complete and irrevocable" are seen in the context of a reasonable effort. We therefore propose the following clarification: The deletion of electronically stored Confidential Information takes place by a deletion of the files or destruction of the data carrier. In the case of electronically stored Confidential Information, a deletion means that the Confidential Information is deleted in such a way which complies with recognised standards. Excluded from this are - in addition to Confidential Information which must be retained - Confidential Information the deletion or return of which is not technically possible, e.g. because it has been stored in a backup file due to an automated electronic backup system for securing electronic data; this also includes the technically necessary provision of master data (e.g. personnel or customer numbers), which is necessary for the storage of the data to create a link to the archived information.	The text of former paragraph 55 (now, paragraph 50) has been clarified to avoid a potential different interpretation of the provisions. On the point related to on-going monitoring, as reported above the word "on-going" has been substituted with the word "regular". On the point related to the deletion of the undertaking data at paragraph 55(d) (former paragraph 60(d)), EIOPA substituted the word "irrevocably" with the word "securely". Furthermore, EIOPA wishes to clarify that complete and secure deletion means deletion compliant with recognised standards (for example, the logical deletion by the cloud service provider of all the data marked for deletion from active systems and expired from backup systems via overwriting and cryptographic techniques) **EIOPA updated the Guidelines accordingly.**
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.	
Most Guidelines address aspects which are to be considered in the best interest of the undertaking before entering cloud service agreements, but 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 to widely waive these Requirements. Otherwise, especially the required registry would be a significant burden and would cause high implementation cost. Some other Guidelines are reasonable, but do not meet the realities of the business environment. For instance, Guideline 13 is hardly enforceable as	**EIOPA partially agrees with the concerns raised by the respondent and updated the Guidelines accordingly.**

Response to the public consultation question	EIOPA Comments
cloud service providers operate worldwide with sub-contractors. In Guideline 15 the mentioned testing of exit plans "where appropriate", should furthermore – if at all – only cover elements on the part of the affected insurance companies. A lesson of the discussion of these draft Guidelines may be to envisage direct regulation of the cloud service providers in the long instead of delegating responsibilities which serve the public good to the undertakings.	
16. Do you have any comments on the impact assessment?	
EIOPA may analyse the option to include cloud providers offering services to supervised industries into the scope of this regulation as it may simplify compliance with regulatory requirements. In addition, options for the EU-wide emission of standards and certificates, e.g. by ENISA, should be elaborated. We would also welcome if EIOPA would thoroughly investigate and make use of synergy potentials, especially with regard to the considerable set of different documentation based on the same assessment. With regard to the policy options analysed in the impact assessment, we would add the following preferences: - 1.2 instead of 1.1 - 2.1 instead of 2.2 - 3.2 instead of 3.1 - 4.2 instead of 4.1 (adjusting the documentation requirements to the requirements of the EBA Guidelines would cause disproportionate cost) - 5.1 instead of 5.2	**EIOPA noted the concerns raised by the respondent** On the suggestion to develop a European supervisory framework for the direct oversight of cloud service providers, EIOPA refers to the Joint Advice of the European Supervisory Authorities to the European Commission on the need for legislative improvements relating to ICT risk management requirements in the EU financial sector[24]. On the point related to the common standards, EIOPA refers to the European Commission's work to develop a set of standardised contractual clauses as part of the FinTech Action Plan and the initiative to develop a SWIPO code of conduct[25]. On policy options 1 and 2, as reported in the impact assessment, EIOPA has chosen the policy option to develop cloud outsourcing Guidelines to timely, answer the increasing market practices of outsourcing to cloud service providers. However, taking into account the feedback to the Public consultation, in the process of reviewing the System of Governance Guideline, EIOPA will evaluate the option to merge these Guidelines with the updated version of the Guidelines on outsourcing. On policy option 3 (The purchase of cloud services falls always under the scope of outsourcing *versus* assessment on the basis of the function outsourced), on the basis of the feedback to the public consultation. EIOPA has defined a third policy option more in line with the respondent feedback. On policy option 4 (Documentation requirements), on the basis of the feedback to the public consultation. EIOPA has defined a third policy option more in line with the respondent feedback and will undertake a broader and comprehensive discussion on how document the outsourcing arrangements when reviewing the System of Governance Guidelines.

[24] The joint advice can be obtained at this link.

[25] Additional information on the SWIPO code of conduct initiative can be obtained at this link.

Response to the public consultation question	EIOPA Comments
	On policy option 5 (Role for college of supervisors in the written notification process before entering into any material cloud outsourcing to cloud service providers critical or important operational functions or activities *versus* the status quo), EIOPA has decided to keep the previous policy choice (i.e. 5.2 "keeping the status quo"). However, taking into account the feedback to the Public consultation, in the process of reviewing the System of Governance Guideline, EIOPA will evaluate the option again.
Annex Y/N	
NO	

Finance Norway, Norway

Response to the public consultation question	EIOPA Comments
General comments on the recommendations Finance Norway supports an additional guidance to the existing Guidelines, in order to provide the needed clarity for institutions should they wish to adopt cloud computing, and fostering supervisory convergence regarding the applicable expectations and processes for the cloud. We think it is essential that fragmentation, as regards financial supervisory regulation and practice is avoided. There is a need to clarify the regulatory framework and the supervisory expectations applied to outsourcing to cloud service providers. An example is the need of a common interpretation of "material cloud outsourcing" among supervisory authorities. In this respect the intention of the recommendations is appreciated. To address the heterogeneity in the supervisory expectations regarding the technical security of cloud computing services, it is important to prevent different interpretations by national supervisors. In order to ensure that the scope of application is sufficiently precise, it is important to have clear definitions. 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 ought to be a risk-based approach to cloud computing, focusing on the outcomes of the recommendations. As the recommendations are aimed at insurance and reinsurance undertakings as well as national supervisory authorities, this could have a negative effect on the transformation of regulated institutions, and may constitute an uneven playing field with other players competing in the same market. On an EU-level, there should be the same guiding principles for contracting between institutions and cloud service providers for all institutions acting in the same market. The General Data Protection Regulation Further consideration should also be given to the General Data Protection Regulation (GDPR), and its Guidelines. Cloud outsourcing includes data transfers between controllers and processors, and as personal data needs to be secured at all times, adequate organizational and technical measures by both controllers and processors are vital. Notification A legal requirement for notification of cloud projects on a case-by-case basis increases the time to market thereby reducing the benefit of using the cloud. Finance Norway thinks that a notification on a case-by-case basis	**EIOPA partially agrees with the concerns raised by the respondent.** General comments on the recommendations Bearing in mind that one of the main purposes of these Guidelines is to provide clarity to the market participants, EIOPA decided to withdraw the use of the term "material outsourcing" sticking to the term "critical or important operational function and activity". For this reason EIOPA deleted the definition of "Material outsourcing" and changed the title of Guideline 7 from "Materiality assessment" to "Assessment of critical or important operational functions and activities." Furthermore, aiming at embedding the principle of proportionality and a risk-based approach on their implementation, EIOPA streamlined the contents of the Guidelines, mainly focusing on outsourcing of critical or important operational functions or activities to cloud service providers. These changes have been done to emphasize EIOPA willingness to focus on substance over form. Moreover, in order to foster the harmonization of the practice related to cloud outsourcing across sectors, EIOPA reviewed the wording of several Guidelines to ensure its alignment (when possible) to the requirements set by the EBA The General Data Protection Regulation EIOPA assessed the Guidelines before and after the consultation and did not identify this as an area that would contradict the GDPR. Notification EIOPA streamlined the content of Guideline 4 "Written notification to the supervisory authorities" clarifying that it is related only to outsourcing of critical or important operational functions or activities by (a) removing the requirement to present a draft copy of the outsourcing agreement (b) aligning the requirements to EBA requirements set by paragraph 54 of EBA Guidelines on outsourcing. In terms of timing, such notification should be performed before entering into a cloud outsourcing arrangement. **EIOPA updated the Guidelines accordingly.**

Response to the public consultation question	EIOPA Comments
ought not to be required either at EU level or by national law or the supervisory practice. 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. Finance Norway therefore proposes to keep these requirements consistent. To avoid unnecessary time, expenses and legal and processual uncertainty, initial notification should be allowed to take place once the cloud initiative is in the production phase.	
Annex Y/N	
YES	

Fund and asset management associations

European Fund and Asset Management Association (EFAMA), Belgium

Response to the public consultation question	EIOPA Comments
EFAMA, the voice of the European investment management industry, welcomes the opportunity to provide its feedback to the EIOPA consultation for the proposal of Guidelines on outsourcing to cloud service providers. EFAMA represents through its 28 member associations, 62 corporate members and 25 associate members more than EUR 25 trillion in assets under management of which EUR 15.6 trillion managed by 60,174 investment funds at end 2017. Close to 32,000 of these funds were UCITS (Undertakings for Collective Investments in Transferable Securities) funds, with the remaining 28,300 funds composed of AIFs (Alternative Investment Funds). Asset management companies in Europe provide services to collective investment undertakings and are covered by their sector-specific regulation, i.e. UCITS Directive[26] and AIFMD[27]. At the same time, a number of asset management companies are part of an insurance group, in which case the parent company is called to ensure the consistent implementation of the requirements deriving from its own sectoral legislation (Solvency II) at the group-wide level. This means that at the group-level Solvency II applies, however it is the sectoral legislation that applies on solo-level, i.e. the level of the asset management company. In this respect, EFAMA wishes to stress the need for a clear guidance in relation to the application of the draft Guidelines for insurance groups. We consider it important to clarify that the EIOPA Guidelines on outsourcing to cloud service providers are first and foremost targeting the internal governance processes of an insurance or reinsurance undertaking. In terms of a consolidated approach the parent institution shall ensure consistency at the group-level, but the provisions applying at solo level for asset managers belonging to an insurance group remain the ones foreseen in the UCITS Directive and AIFMD. Any different approach would lead to regulatory inconsistencies such as requesting asset management companies-subsidiaries in insurance groups to apply two different sets of rules as regards their outsourcing arrangements or to disregard their existing sector-specific regulatory framework, which they are not entitled to do. Moreover, the EIOPA Guidelines do not reflect the specificities of the asset management business model and their sector specific-requirements. In case there may be a need to further develop a common understanding of similar outsourced activities across the spectrum of financial entities and based on the ESA's Joint Advice on the need for legislative improvements relating to ICT risk management requirements in the EU financial sector[28], it would be on ESMA to make the necessary clarifications and precisions for securities markets legislation. **In this context, we call EIOPA to ensure that the application of these Guidelines is not foreseen at solo level for asset management companies that are part of an insurance group. This should be indicated in paragraph 2 of the Guidelines referring to the scope both for insurance undertakings and mutatis mutandis for groups.**	**EIOPA agrees with the concerns raised by the respondent and clarified the text of the Guidelines.**
Annex Y/N	
YES	

[26] Directive 2009/65/EC of the European Parliament and of the Council of 13 July 2009 on the coordination of laws, regulations and administrative provisions relating to undertakings for collective investment in transferable securities (UCITS)

[27] Directive 2011/61/EU of the European Parliament and of the Council of 8 June 2011 on Alternative Investment Fund Managers and amending Directives 2003/41/EC and 2009/65/EC and Regulations (EC) No 1060/2009 and (EU) No 1095/2010

[28] https://www.esma.europa.eu/sites/default/files/library/jc_2019_26_joint_esas_advice_on_ict_legislative_improvements.pdf

BVI Bundesverband Investment und Asset Management e.V (BVI), Germany

Response to the public consultation question	EIOPA Comments
BVI[29] members are asset managers providing management services to collective investment undertakings such as UCITS or AIF. Most of them are investment management companies within the meaning of Directive 2009/65/EC ("UCITS Directive") or Directive 2011/61/EU ("AIFMD") for which the Solvency II Directive does not apply and sector-specific requirements are in place. However, for some of them the consultation at hand can be relevant if they are part of an insurance group. We are concerned about the scope defined under paragraph 2 of the draft Guidelines that is focused on "both individual (insurance) undertakings and mutatis mutandis for groups". The latter reference could be misunderstood in the sense that the Guidelines should also apply directly on solo-level to as-set management companies being part of an insurance group. This would lead to the situation that these companies would be required to implement two different regimes on solo level, the regime of the UCITS Directive/AIFMD and the EIOPA Guidelines as an outcome of the Solvency II Directive. These requirements differ in key aspects such as functions which could be outsourced, including specific conditions for delegation of functions into third countries and, in particular, the outsourcing process including the content of outsourcing agreements and controlling process. Moreover, the outsourcing requirements proposed by the EIOPA in its Guidelines are not designed to reflect these sector-specific requirements and specific business models of asset management companies. In view of financial stability, there may be a need for further development of a common understanding of outsourced business activities in the insurance sector and for issuing EIOPA Guidelines on internal governance processes regarding the risks insurance undertakings are or might be exposed to, also in a group context. However, the legal mandate given to EIOPA does not involve issuing Guidelines with regard to the application of Solvency II rules to subsidiaries of insurance undertakings for which sector-specific requirements apply. In this context, we refer to the Joint Advice[30] of the ESAs on the need for legislative improvements relating to ICT risk management requirements in the EU financial sector that makes a precise distinction between banking, insurance and securities markets legislation. EBA has also clarified in its final report[31] on EBA Guidelines on outsourcing arrangements that firms subject to the UCITS Directive or the AIFMD are not in scope on an individual level. We therefore request EIOPA to explicitly clarify in their Guidelines that investment management companies licensed under the UCITS Directive or AIFMD and being part of an insurance group are out of the scope of the proposed Guidelines and are not required to implement all these requirements drafted in the Guidelines on solo-level.	**EIOPA agrees with the concerns raised by the respondent and clarified the text of the Guidelines.**
Annex Y/N	
YES	

[29] BVI represents the interests of the German fund industry at national and international level. The association promotes sensible regulation of the fund business as well as fair competition vis-à-vis policy makers and regulators. Fund companies act as trustees in the sole interest of the investor and are subject to strict regulation. Funds match funding investors and the capital demands of companies and governments, thus fulfilling an important macro-economic function. BVI's more than 100 members manage assets of some 3 trillion euros for private investors, insurance companies, pension and retirement schemes, banks, churches and foundations. With a share of 22% in the EU Germany represents the largest fund market as well as the second fastest growing market in the EU. BVI's ID number in the EU Transparency Register is 96816064173-47. For more information, please visit www.bvi.de/en.

[30] Available under the following link: link

[31] Cf. EBA/GL/2019/02, 25 February 2019, page 78.

Other industry associations

The Polish Chamber of Information Technology and Telecommunications, Poland

Response to the public consultation question	EIOPA Comments
1. Is the scope of application provided appropriate and sufficiently clear?	
YES	NA
2. Is the set of definitions provided appropriate and sufficiently clear?	
YES	NA
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?	
YES	NA
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?	
One of the most visible differences between outsourcing and cloud services is the self-provisioned and self-managed by the user (see the definition: "that can be rapidly provisioned and released with minimal management effort or service provider interaction". In the very general sense cloud services are subset of outsourcing, however, for the purpose of this recommendation it shall be communicated very clearly. The reason is in list of formal requirements level from undertakings to cloud vendor. It shall be required from cloud vendor to provide clear and public information on how the requirements are met, however, there shall be no specific obligations to provide case by case tailored documents, agreements etc. Compare also: Guideline 3, Written policy on outsourcing to cloud providers	**EIOPA noted the concerns raised by the respondent.**
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?	
In case of using cloud services it shall be the basic practical checklist of requirements provided by regulator, which can be publicly available for all stakeholder; the list shall be coordinated on European level to avoid the different scope of requirements for over the border services; the local regulator can also check (in regular way) the most common and popular cloud services against that checklist – the list of such services shall be available to undertakings (this is approach started by government of New Zealand for using cloud services in administration) – compare with Guideline 4 of what shall be delivered to regulator; the undertakings shall be responsible for making the risk assessment of the implementation, documentation (accountability, see Guideline 5) and exit strategies.	**EIOPA noted the concerns raised by the respondent.**
5b. Is the Guideline on written policy consistent to the market best practices on defining the policy for general outsourcing?	
See comments to question 5a	NA
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?	

Response to the public consultation question	EIOPA Comments
NO. no comments	**EIOPA noted the concerns raised by the respondent.**
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?	
- Art. 23 d) – this type of information can be trading secret and it does not bring a lot of value to regulator – proposal: remove this point - Art 23 e) – audits when applicable or information on audits provided by independent auditors - Art 23 f) – proposal: "list of the names or availability of the names of significant sub-outsourcers"; this better reflects how the public cloud services are organized, where cloud vendors are providing the list of sub-outsourcers (sub processors) available on line - Art 23 g) – more clearance of terms needed. Is that the availability level or latency level? Or, is that fulfilling the requirements of NIS Directive for Digital Services Providers (e.g. from 151/2018) - Art 23 h) – proposal" availability of the proof of business continuity plan"; better reflects the cloud services, where proof of business continuity can be achieved e.g. with compliance with ISO 22301 – see also art. 27 Please compare the last two comments to art. 29, clearly pointing at international standards	**EIOPA partially agrees with the concerns raised by the respondent.** EIOPA has streamlined the content of the Guideline 5 in order to make it more principle and risk based by removing the requirements for keeping a register and requiring the undertaking to record information of their cloud outsourcing arrangements. Furthermore, EIOPA has defined, as minimum requirement, a set information to be recorded only for critical or important operational functions outsourced to cloud service providers. This set of information is aligned to the one required by the EBA Guidelines on Outsourcing. As a result, several changes requested by the stakeholders have been included in the Guideline: - On former paragraph 23(d), being the information on budget costs a possible metric of the significance of the provider, kept the requirement to record it. Moreover, in order to clarify the purpose, EIOPA aligned the wording to the one used by the EBA in its Guidelines on outsourcing; - On former paragraph 23(e), EIOPA decided to keep the requirement to have a consistent approach with the one taken by the EBA; - On former paragraph 23(f), EIOPA changed the wording of the provision. Undertakings can make reference to the list of sub-contractors as provided in the cloud service providers website; - On the former paragraph 23(g), it is made reference to the availability level which can be assessed by each individual undertaking, for example as part of the definition of its own business continuity objectives during their Business Impact Analysis; - Former paragraph 23(h) has been removed. **EIOPA clarified the text of the Guidelines accordingly.**
7b. What can be other approaches to ensure a proper and sound holistic oversight of cloud outsourcing?	
See comments to question 7a	NA
8. Are the documentation requirements appropriate and sufficiently clear?	
See comments to question 7a	NA
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. NO COMMENTS	**EIOPA noted the concerns raised by the respondent**
10. Is the content of Guideline on risk assessment of cloud outsourcing appropriate and sufficiently clear?	
Art. 29 g) and h) the local regulator should provide the clear guidance on political stability and security situation in particular countries to provide common strategy to all undertakings; this shall not be part of the work for	**EIOPA partially agrees with the concerns raised by the respondent.** - On former paragraph 29(g), now paragraph 31(b iv), EIOPA kept the wording already foreseen by the EBA Guidelines on Outsourcing to

Response to the public consultation question	EIOPA Comments
insurance companies which may not have the information or proper assessment Art. 29 i) – this is covered in exit plans	facilitate the creation of standards of information related to legal, compliance and political stability of third countries to be used for pre-outsourcing risk assessments. - On former paragraph 29(h), now paragraph 31(b v), the content of the provision has been simplified. - On former paragraph 29(i), now paragraph 31(b vi), the content of the provision has been simplified. Furthermore, EIOPA wishes to specify that knowing how much of an undertaking outsourcing is concentrated into one or more (cloud) service providers is a useful information that the decision making body should weigh in the risk assessment to decide whether or not outsource to that specific cloud service provider the specific service. The Guidelines do not preclude the outsourcing to cloud service providers with market dominance (or that is not easily substitutable). **EIOPA clarified the text of the Guidelines accordingly.**
11. Are the contractual requirements for material outsourcing appropriate and sufficiently clear?	
Art. 35 – the documentation as described can be provided not only by cloud vendor, but also by cloud broker. Art. 35 the list of requirement: basing on characteristics of cloud services and constant changes of the service the better solution is availability of the required information, not one-time picture of the compliance Art. 35 g) the location of the data storing shall based and be responsibility of undertaking ("self-provisioning of the cloud")	**EIOPA noted the concerns raised by the respondent**
12. Are the criteria provided to set the contractual requirements for non-material outsourcing appropriate and sufficiently clear?	
see comments to question 11	**NA**
13. Are the Guideline on access and audit rights appropriate and sufficiently clear	
The proposal: the change of order! Basing on hyperscale character of cloud services we propose to use provision of art. 44 terms first and only if it is not appropriate or not enough then undertaking shall execute the audit as described in articles 40-43 and 47.	**EIOPA noted the concerns raised by the respondent** At Guideline 11, in order to foster the development of European-wide standards in the area of auditing cloud services for financial institutions, EIOPA aligned the conditions to use third party certifications or audit reports to the ones set by the EBA Guidelines on outsourcing (paragraphs 92-93). These conditions include, in case of outsourcing of critical or important operational functions or activities to cloud service providers, the requirement for the undertakings to not rely solely on third-party certifications and reports over time. This means that undertakings should not simply assume that receiving a certificate or a report is enough assurance that the cloud service is being provided in accordance with their legal, regulatory and risk management

Response to the public consultation question	EIOPA Comments
	obligations. If an undertaking elects to use third party certifications as audit tool, such undertaking should assess the adequacy of the information in these certifications against its own requirements and make follow-up enquiries to the cloud service providers if necessary (which might include the performance of on-site audits).
14. Are the provisions set by this Guideline for security of data and systems appropriate and sufficiently clear?	
Art. 50 f) the provision shall be clearly related to GDPR and Free Flow of non-Personal Data in EU. The data residency shall be limited only in specific situation. Art. 50 g) not clear if monitoring of information from cloud service provider or availability of the tools from cloud vendor are enough?	**EIOPA agrees with the concerns raised by the respondent** - On former paragraph 50(f), EIOPA removed the reference to the definition of a data residency policy and substituted it with a more principle based instruction; - On the question related to former paragraph 50(g), now paragraph 49(i), EIOPA wishes to specify that the adequacy of the tools to be used by the undertaking to perform the regular monitoring of the fulfilment of the control systems implemented by the cloud service provider should be evaluated on a case by case basis. This includes the monitoring tools provided by the cloud service providers. **EIOPA clarified the text of the Guidelines accordingly.**
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.	
General comment: There is a need for clear and practical cloud guidance from regulator assuming that outsourcing and cloud services are insurance undertakings' response to growing efficiency, response to market needs and security. If, however, the requirements and formal procedures to enter cloud services will be complex, time and effort consuming – the transition process will slow down. But there is even bigger risk to be taken into account. If the requirements for "going cloud" and level of formality will be significantly higher than for on premise implementation – it will stop the process. The guidance shall be in par with on premise requirements. Example: the business continuity requirements from cloud service provider cannot be higher than business continuation	**EIOPA noted the concerns raised by the respondent**
16. Do you have any comments on the impact assessment?	
NA	NA

Insurance and reinsurance undertakings and groups

Allianz Group, Germany

Response to the public consultation question	EIOPA Comments
1. Is the scope of application provided appropriate and sufficiently clear?	
The proposed Guidelines concern the application of general outsourcing rules (described in the Guidelines on the System of Governance) to cloud services. They are to some extent redundant (with more or less variation) with the existing rules of law and the Guidelines on the System of Governance. Many of the proposed Guidelines are so general that they could apply to all outsourcings, not only to outsourcing to cloud providers. We would therefore question the necessity for EIOPA Guidelines on the specific topic of outsourcing to cloud service providers. We consider the general governance rules and their interpretation by the Guidelines on the System of Governance, as fully sufficient. If at all considered necessary, the existing Guidelines on the System of Governance should be supplemented. This would avoid a lot of confusion and be more efficient. We note that also EBA has taken this approach by integrating its Recommendation on Cloud Outsourcing, published in December 2017, into its revised Guidelines on Outsourcing Arrangements (version of February 2019) and repealing the former. Overall, if the rationale to distinguish between general outsourcing and outsourcing to cloud service providers is concentration risk, we believe it would be much more effective to address concentration risks at the level of cloud service providers who master the technology where risk concentration manifests and not at the level of insurers. Otherwise regulated undertakings would be at a disadvantage in using state of the art technologies. Moreover, if the risk materializes the consequences would not be confined to the financial sector. This point was already noted by the ESAs in their Joint Advice to the EU Commission on ICT Risk Management (April 2019). We support the ESAs proposal for an appropriate oversight framework for Cloud Service Providers when they are critical service providers to relevant entities. The draft Guidelines specify that they should also be applicable mutatis mutandi at the level of the group. While this may follow from Art. 246 and 49 of the Solvency II Directive, for the sake of clarity and to avoid redundant or even conflicting requirements, the Guidelines should specify that sectoral requirements should apply to group companies of other financial sectors.	**EIOPA noted the concerns raised by the respondent.** As reported in the impact assessment, EIOPA has chosen the policy option to develop cloud outsourcing Guidelines to timely, answer the increasing market practices of outsourcing to cloud service providers. However, taking into account the feedback to the Public consultation, in the process of reviewing the System of Governance Guideline, EIOPA will evaluate the option to merge these Guidelines with the updated version of the Guidelines on outsourcing. Furthermore, EIOPA wishes to clarify that, in the process of reviewing the Guidelines on the basis of the feedback to the public consultation, EIOPA streamlined the contents of the Guidelines, mainly focusing on outsourcing of critical or important operational functions or activities to cloud service providers. These changes have been done to emphasize EIOPA willingness to focus on substance over form On the last point related to the application of these Guidelines at solo level by group subsidiaries belonging to other financial sectors, EIOPA agrees with the concern raised by the respondent and clarified the text of the Guidelines specifying that without prejudice to Article 246 of Directive 2009/138/EC and EIOPA Guidelines on System of Governance, the entities subject to other sectoral supervisory requirements, which are part of a group, are excluded by the scope of application of these Guidelines at solo level as they shall follow the sectoral specific regulatory requirements as well relevant guidance issued by the European Securities and Markets Authority and the European Banking Authority.
2. Is the set of definitions provided appropriate and sufficiently clear?	

Response to the public consultation question	EIOPA Comments
We question the necessity for EIOPA Guidelines on the specific topic of outsourcing to cloud service providers. We consider the general governance rules and their interpretation by the Guidelines on the System of Governance, as fully sufficient. If at all considered necessary, the existing Guidelines on the System of Governance should be supplemented. This would avoid a lot of confusion and be more efficient. We note that also EBA has taken this approach by integrating its Recommendation on Cloud Outsourcing, published in December 2017, into its revised Guidelines on Outsourcing Arrangements (version of February 2019) and repealing the former. Definitions should be identical with and limited to those contained in the EBA Guidelines on Outsourcing (Guideline 2, #12 et seq. (Definitions)). With respect to the added definitions, we see the following problems: 1. Definition of "service provider" and "cloud service provider": Not every use of cloud services is an outsourcing. Many cloud services used by insurance undertakings will not meet the criteria for outsourcing (i.e. materiality, permanence and relation to insurance business). Therefore, the definition of "service provider" and "cloud service provider" should not refer to "outsourcing arrangements" or "outsourced process", since it must not include (cloud) service providers that provide cloud services not qualifying as outsourcing. 2. The definition of "significant sub-outsourcer" contains a criteria for "significance" that can be confused with the criteria for the (sub-) outsourcing of critical or important operational functions or activities pursuant to Art. 274 (3) SII Delegated Regulation. There should not be independent criteria to qualify the criticality or importance of an sub-outsourced function or activity. Rather, the general criteria should apply. 3. Neither level 1 nor level 2 text use the term "material outsourcing", but speak of "outsourcing of critical and important functions and services". EIOPA should use this terminology rather than introduce new terms like "material outsourcing" as this will lead to confusion. 4. The definition of the cloud services should also be aligned and in correlation with the definition of "cloud computing service" in Art. 4 (19) of the NIS Directive.	**EIOPA partially agrees with the concerns raised by the respondent.** On the decision to issue specific Guidelines on cloud outsourcing, please refer to the EIOPA comments to the response to Question 1. On the definitions: Service provider, according to Article 13 (28) of Solvency II Directive, "*outsourcing means an arrangement of any form between an insurance or reinsurance undertaking and a service provider, whether a supervised entity or not, by which that service provider performs a process, a service or an activity, whether directly or by sub-outsourcing, which would otherwise be performed by the insurance or reinsurance undertaking itself*". Notwithstanding the above, EIOPA agrees with the respondent that not all the arrangements with third parties are outsourcing. There are two type of arrangements with third parties: 1) Services which are not outsourcing (for example, non-recurrent activities and purchases of goods – including software licences – are not considered as outsourcing arrangements) and 2) Services, which are outsourcing. Among the services which are outsourcing there is a distinction between: - outsourcing of critical or important operational functions (which includes, but is not limited to, insurance and reinsurance processes and activities, functions as defined by Solvency II art. 13(29), provisioning of on-going day to day systems maintenance or support, investment of assets or portfolio management, etc.) - outsourcing of non-critical, non-important operational functions (i.e. less material). In light of the above, the definition of service provider and the definition of cloud service provider have been clarified. Significant sub-outsourcer on the basis of the feedback received and in order to have market consistency the definition has been deleted Material outsourcing, on the basis of the feedback received and bearing in mind that one of the main purposes of these Guidelines is to provide clarity to the market participants, EIOPA decided to withdraw the use of the term "material outsourcing" sticking to the term "critical or important operational function and activity". The definition has been deleted Cloud services, in order to have market consistency the definition has been kept aligned to the one used in the EBA Guidelines on outsourcing. No changes have been made.

Response to the public consultation question	EIOPA Comments
	EIOPA updated the Guidelines accordingly.
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?	
If the Guidelines would cause a change in supervisory practice by the national competent authority (NCA), any such change should not affect existing arrangements. Existing arrangements have, in certain jurisdictions, been authorized by the NCA. A change in supervisory practice (other than a change of law), however, can never justify the withdrawal of such granted authorization. It should be relevant only for new arrangements.	**EIOPA noted the concerns raised by the respondent.** The authorisations already granted by National Competent Authorities are still valid. However, to ensure that a proper management of cloud outsourcing arrangements according to these Guidelines is in place, the pre-existing arrangements related to critical or important operational functions or activities should be reviewed.
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?	
There should not be an assumption that every cloud service qualifies as outsourcing. Rather, in accordance with general criteria, the assessment and classification should be made on the basis of the relevant circumstances. Such circumstances have great variation, so that an assumption is not appropriate. Furthermore, the Guidelines should not set out general criteria for the outsourcing classification of cloud services if such criteria are not specific to cloud use. The proposed Guidelines introduce new general criteria that could be applicable to all outsourcings, but are not contained in the Guidelines on the System of Governance, nor any rule of law, and, additionally, deviate from the definition set forth in Art. 13 (28) of the Solvency II Directive.	**EIOPA partially agrees with the concerns raised by the respondent.** The determination of whether (or not) the purchase of cloud services fall into the scope of outsourcing is paramount to a successful and coherent application of these Guidelines. The assessment to this application is responsibility of the undertakings and should be carried out by applying the criteria provided in Guideline 1 and in the regulatory obligations listed in the introduction of these Guidelines. On the respondent request to eliminate the sentence "as a rule outsourcing should be assumed" from the Guideline, in light of the above, EIOPA deleted that sentence. **EIOPA updated the Guidelines accordingly**
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?	
We see no need for Guideline 3: Criteria a. to f. are contained in Art. 274 of the Solvency II Regulation and not specific to cloud services. Also, when applied to cloud computing services, we do not see that responsibilities or processes laid out in the existing written outsourcing policies would have to be changed or complemented in any way with respect to such criteria. Rather, the outsourcing of cloud computing should follow the general outsourcing process so as to achieve consistent governance.	**EIOPA partially agrees with the concerns raised by the respondent.** EIOPA has decided to keep the Guideline clarifying its application. For this reason, as the Solvency II principles on outsourcing are still valid for cloud, with reference to the update of internal policies and procedures, multiple solutions are at disposal for undertakings: 1) development – where needed – of a dedicated cloud outsourcing policy; 2) complement - where needed – the undertaking outsourcing policy and the other relevant internal policies (for example the information security policy) to take into account the specificities of outsourcing to cloud service providers; and 3) if the undertaking current policies cover the elements described in these Guidelines, there is no need to update.

Response to the public consultation question	EIOPA Comments
	EIOPA updated the Guidelines accordingly.
5b. Is the Guideline on written policy consistent to the market best practices on defining the policy for general outsourcing?	
See answer above	NA
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?	
Notification requirements should only apply where stipulated in national law implementing the Solvency II Directive. Assuming that what EIOPA refers to as "material cloud outsourcing" qualifies as outsourcing of critical or important functions or activities within the meaning of Art. 274 SII Delegated Regulation, there is no need to state that the notification requirement set forth in Art. 49 (3) of the SII Directive applies. (Not relevant in practice, but a dogmatic inconsistency: Art. 49 (3) does not require "written" notification.). The information items listed in lit. d) on other group undertakings making use of the cloud service, should only be required in the notification to the group supervisor. It may not be available or not be of relevance at local level.	**EIOPA partially agrees with the concerns raised by the respondent.** The content of Guideline 4 which is related only to outsourcing of critical or important operational functions or activities has been streamlined by: (a) removing the requirement to present a draft copy of the outsourcing agreement (b) aligning the requirements to the EBA requirements set by paragraph 54 of the EBA Guidelines on outsourcing to ensure market consistency. On the point related to the "dogmatic inconsistency", EIOPA agrees with the respondent that the Article 49(3) does not require a written notification but simply to notify the supervisory authorities. However, to ensure consistency with the wording used in the System of Governance Guidelines (Guideline 64 "Written notification to the supervisory authority"). As part of the review of the Guideline, the former paragraph 18(d) has been removed and only included in the information that should be recorded for critical or important operational functions or activities. **EIOPA updated the Guidelines accordingly.**
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?	
While the documentation of the information set forth in the proposed Guidelines may be part of good governance, and thus already be required by general rules and for all types of outsourcing, we do not see a need to make a specific requirement for a "register". In which form and place the information is stored should be left to the undertakings' own organizational discretion. The list of information proposed by EIOPA contains too much detail. Information should be limited to what is required to meet notification and reporting requirements. Any more detail would create unnecessary bureaucratic burden without adding any value. For example, data fields, such as the corporate registration number, seem redundant (if name of the company and address is available) and it is difficult to imagine under which circumstances this information would actually be required	**EIOPA partially agrees with the concerns raised by the respondent.** EIOPA has streamlined the content of the Guideline 5 in order to make it more principle and risk based by removing the requirements for keeping a register and requiring the undertaking to record information of their cloud outsourcing arrangements. Furthermore, EIOPA has defined, as minimum requirement, a set information to be recorded only for critical or important operational functions outsourced to cloud service providers. This set of information is aligned to the one required by the EBA Guidelines on Outsourcing. For outsourcing to cloud service providers on non-critical non-important operational functions or activities, the level of detail of the information to be recorded should be determined by the undertakings on a risk-based approach.

Response to the public consultation question	EIOPA Comments
	EIOPA updated the Guidelines accordingly.
7b. What can be other approaches to ensure a proper and sound holistic oversight of cloud outsourcing?	
No comment	NA
8. Are the documentation requirements appropriate and sufficiently clear?	
We strongly recommend remaining only in the strict perimeter of notifications obligation specified in the Solvency II Directive and under the clear instructions of the national authorities which only requires to notify a critical or important outsourcings (and therefore not all cloud outsourcings).	**EIOPA noted the concerns raised by the respondent.**
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?	
The concept of "outsourcing of critical or important functions or activities" as set forth in Art. 49 (2) and (3) of the Solvency II Directive and Art. 274 (3) of the SII Delegated Regulation should not be changed by any EIOPA Guidelines, neither with respect to cloud services nor to other services. A clear reference to those legal provisions is necessary and no further criteria (e.g. "whether the cloud outsourcing is materially affecting the risk profile of the undertaking"), potentially extending the legal definition, should be introduced. Likewise, stating that undertakings should consider "always" as material all the outsourcing of critical or important operational functions to cloud providers suggests that the concept of "materiality" is broader than the concept of a 'critical or important operational function', which would not be in line with the SII Directive.	**EIOPA partially agrees with the concerns raised by the respondent.** On the use of the term "material" instead of the term "critical or important", as reported above, bearing in mind that one of the main purposes of these Guidelines is to provide clarity to the market participants, EIOPA decided to withdraw the use of the term "material outsourcing" sticking to the term "critical or important operational function and activity". **EIOPA updated the Guidelines accordingly.**
10. Is the content of Guideline on risk assessment of cloud outsourcing appropriate and sufficiently clear?	
The draft Opinion does not specify under which regulation undertakings are required to provide the supervisory authority with a cost-benefit analysis in their risk assessment and a regular update of the risk assessment. The Opinion should not create new requirements. The list of those items does not highlight what the specificities of the control of cloud services are, compared to the items covered in risk assessment for other outsourced services.	**EIOPA noted the concerns raised by the respondent.**
11. Are the contractual requirements for material outsourcing appropriate and sufficiently clear?	
It should be clarified that regarding the cloud services pricing model as proposed in Guideline 10, No 35 d, a reference in the contract to a pricing model description which is available online is sufficient. Currently all major cloud service providers rely on pricing model descriptions which are available only online and which are subject to changes upon notice. Undertakings are usually negotiating discounts on such price lists which are publically available. A	**EIOPA partially agrees with the concerns raised by the respondent.** EIOPA reviewed extensively the text of the Guideline 10 to ensure a better inclusion of the principle of proportionality. In light of this, EIOPA:

Response to the public consultation question	EIOPA Comments
requirement to include the pricing model in the contract without the possibility to reference online terms would require a massive change of the current business model of cloud service providers, which is simply not realistic. While we agree that service levels should be agreed that include quantitative and qualitative performance targets, it should not be a requirement that these are directly measurable by the undertaking. We are of the opinion that it must be possible to rely on the reporting provided by the cloud service provider, subject to the ability of the undertaking to audit such reporting at any time. Further, we do not consider it appropriate to require a clause that stipulates whether the cloud service provider should take mandatory insurance against certain risks. This should be subject to the outcome of the risk assessment and should not be a general requirement.	(1) reviewed the scope of application of the Guideline which will be applicable only in case of cloud outsourcing of critical or important operational functions or activities; (2) clarified the relationship between this Guideline and the requirements set by Directive 2009/138/EC and Commission Delegated Regulation (EU) No 2015/35 by eliminating the former paragraphs 36 and 37. Furthermore, bearing in mind the possible complexities of its implementation in case of misalignments between the content of this Guideline and of the one set by the EBA on the same subject, EIOPA further aligned the wording of this Guideline to the EBA requirements set by paragraph 75 of the EBA Guidelines on outsourcing. In light of this, on the specific requests to amend elements of the Guidelines, EIOPA: - agrees with the respondent being up to the contractual parties to consider mandatory insurance for the outsourced activities and whether this issue should be addressed in the outsourcing agreement. - to avoid unnecessary complexities in understanding how to apply the Guideline and to leverage on implementation already carried out by several cloud service providers to comply to the EBA Guidelines on the same subject, EIOPA kept the same wording as defined by the EBA Guidelines on data localisation and on performance target. **EIOPA updated the Guidelines accordingly.**
12. Are the criteria provided to set the contractual requirements for non-material outsourcing appropriate and sufficiently clear?	
NO COMMENT	NA
13. Are the Guideline on access and audit rights appropriate and sufficiently clear?	
We think that, in general, access and audit rights vis-à-vis a digital services providers would be more effective if in favour of the authorities competent under the NIS Directive. Inclusion of cloud service providers providing services for supervised industries into the NIS Directive should be envisaged. As for Germany, the „Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSIG)" with its „Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSIGesetz (BSI-KritisV)" already requires cloud infrastructures to comply with standards and provides for certain certifications. These standards and certificates should be usable when undertakings have to audit their cloud service providers. These kinds of certifications should also be available on an EU-level, e.g. provided by ENISA.	**EIOPA noted the concerns raised by the respondent** On the points related to the Guidelines, EIOPA clarified the scope of application of the Guideline, which will be applicable only in case of cloud outsourcing of critical or important operational functions or activities. Furthermore, in order to foster the development of European-wide standards in the area of auditing cloud services for financial institutions, EIOPA aligned the conditions to use third party certifications or audit reports to the ones set by the EBA Guidelines on outsourcing (paragraphs 92-93). These conditions include, in case of outsourcing of critical or important operational functions or activities to cloud service providers, the requirement for the undertakings to not rely solely on third-party certifications and reports over time. This means that undertakings should not simply assume that receiving a certificate or a report is enough assurance that the cloud service is being provided in accordance with their legal, regulatory and risk management

Response to the public consultation question	EIOPA Comments
The Guidelines require a variety of different documents that sometimes require similar assessments. This causes even more complex and time consuming paperwork for undertakings without any clear benefit. In addition, as long as it is not clear under which conditions insurers can rely on third-party reports or pooled audits, they have to do on-site visits themselves or need a representative at the pooled audits. Since cloud service providers charge their clients for on-site visits and audits, this leads to costs that might be affordable for large insurance companies. However, it might refrain smaller insurance companies from using cloud services and thus limit competition among them.	obligations. If an undertaking elects to use third party certifications as audit tool, such undertaking should assess the adequacy of the information in these certifications against its own requirements and make follow-up enquiries to the cloud service providers if necessary (which might include the performance of on-site audits).
14. Are the provisions set by this Guideline for security of data and systems appropriate and sufficiently clear?	
As mentioned above, it would be preferable if those obligations were directly born by cloud services providers and not by insurance companies. The regulations of cloud services providers should be reviewed. For insurance companies ongoing controls are very difficult to carry out e.g. network traffic is not under the responsibility of the insurance companies.	**EIOPA noted the concerns raised by the respondent**
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 COMMENT	NA
16. Do you have any comments on the impact assessment?	
Inclusion of cloud service providers providing services for supervised industries into the NIS Directive should be envisaged. As for Germany, the „Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSIG)" with its „Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSIGesetz (BSI-KritisV)" already requires cloud infrastructures to comply with standards and provides for certain certifications. These standards and certificates should be usable when undertakings have to audit their cloud service providers. These kinds of certifications should also be available on an EU-level, e.g. provided by ENISA. The Guidelines require a variety of different documents that sometimes require similar assessments. This causes even more complex and time consuming paperwork for undertakings without any clear benefit.	**EIOPA noted the concerns raised by the respondent**
Annex Y/N	
NO	

Mutuelle Bleue, France

Response to the public consultation question	EIOPA Comments
1. Is the the scope of application provided appropriate and sufficiently clear?	
YES	NA
2. Is the set of definitions provided appropriate and sufficiently clear?	
YES	NA
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?	
YES	NA
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?	
YES	NA
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?	
Donner des exemples TRANSLATION: Give examples	**EIOPA disagrees with the concerns raised by the respondent.** Considering that some examples have already been included in the explanatory text of the EIOPA Guidelines on system of governance, EIOPA has decided to not include in the Guidelines examples of cloud services that are not to be considered as outsourcing. **No changes were made to the Guidelines.**
5b. Is the Guideline on written policy consistent to the market best practices on defining the policy for general outsourcing ?	
Pratiques informatiques ne sont pas forcément orientées sur l'intégralité des points évoquées dans les lignes directrices TRANSLATION: IT practices are not necessarily oriented towards all the points mentioned in the Guidelines	**EIOPA noted the concerns raised by the respondent.**
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?	
YES	NA
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	**EIOPA noted the concerns raised by the respondent.**
7b. What can be other approaches to ensure a proper and sound holistic oversight of cloud outsourcing?	
Surveillance réseau constante, du point de vue de l'utilisateur et du serveur TRANSLATION: Constant network monitoring, from the point of view of the user and the service provider	**EIOPA noted the concerns raised by the respondent.**
8. Are the documentation requirements appropriate and sufficiently clear?	
Implémentation à faire par des directions informatiques des lignes directrices TRANSLATION Implementation to be done by IT directorates of Guidelines	**EIOPA noted the concerns raised by the respondent.**

Response to the public consultation question	EIOPA Comments
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?	
YES	NA
10. Is the content of Guideline on risk assessment of cloud outsourcing appropriate and sufficiently clear?	
YES	NA
11. Are the contractual requirements for material outsourcing appropriate and sufficiently clear?	
YES	NA
12. Are the criteria provided to set the contractual requirements for non-material outsourcing appropriate and sufficiently clear?	
YES	NA
13. Are the Guideline on access and audit rights appropriate and sufficiently clear	
YES	NA
14. Are the provisions set by this Guideline for security of data and systems appropriate and sufficiently clear?	
YES	NA
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.	
YES	NA
16. Do you have any comments on the impact assessment?	
No comment	NA
Annex Y/N	
NO	

Irish Life Group, Ireland

Response to the public consultation question	EIOPA Comments
1. Is the scope of application provided appropriate and sufficiently clear?	
No, see document attached. **Excerpt from Irish Life Group's document** Introduction Irish Life Group firmly agrees with the principle of proportionality as set out in point 3 within the introduction to the Guidelines. It is our view that it is of critical importance that competent authorities across all Member States are aligned with regards to this principle and apply it consistently across all jurisdictions. To allow wide interpretations on proportionality would potentially create regulatory arbitrage and increase complexity across the Internal Market. Some criteria that could be considered in assessing the proportionality of each arrangement would be: - The materiality and criticality of the activity cloud is being used to support to the overall activities of provider. - Substitutability to replace the cloud provider in the event of an issue arising either through bringing the activity back in house or sourcing an alternative provider. - The availability of alternative providers in the market. - Benefits and risks associated with the cloud arrangement in terms of meeting customer commitments and regulatory requirements. - Where the cloud infrastructure in question is using public or private cloud. - The type of cloud arrangement, i.e. whether it is IaaS, PaaS or SaaS. We feel it is very important for EIOPA to acknowledge that the wide range of types of cloud arrangements possible means that a single governance standard is not appropriate for them all. In addition, Irish Life Group would have a concern that a challenge may arise where the current Guidelines overlap with other legislative and regulatory requirements, where the principle of proportionality is not explicitly called out. For example EIOPA Explanatory Text supporting its Guidelines on System of Governance notes that: "*in determining whether an outsourced function or activity is critical or important the undertaking has to take into account any definition or list of such functions or activities provided under national law or national administrative interpretation*". Where these lists under national law or national administrative interpretation are not prefixed with the notion of proportionality they can never hope to	**EIOPA noted the concerns raised by the respondent** The application of the principle of proportionality in the context of cloud outsourcing should not differ from the application of the same principle in the context of outsourcing in general. EIOPA therefore decided to not further define the principle of proportionality in these Guidelines. On the example described by the respondent, EIOPA wishes to clarify that the "criteria that could be considered in assessing proportionality of each arrangement" have been incorporated in Guideline 8 (Risk assessment). On the tiered approach used by Irish Life, EIOPA wishes to clarify that such approach has been incorporated in Guideline 7.

Response to the public consultation question	EIOPA Comments
capture any degree of proportionality when considered across different undertakings and the individual scale and complexity of each individual outsourcing arrangement. This can lead to binary, non-risk sensitive categorization of arrangements as critical or important and impose excessive governance expectations. E.g. in EIOPA Explanatory Text supporting its Guidelines on System of Governance, 'provision of data storage' is stated as an example of a critical or important function. This does not consider the nature, scale and complexity of the risks attaching to the specific data set being stored, storage location, etc. Proportionality is of additional importance in the context of cloud services arrangements which are in constant development with undertakings needing to apply risk-sensitive proportionality to the application of the Guidelines in the context of agile initiatives development. The industry is increasingly responding to the threat of disruption through innovation labs and agile proof of concept projects. Supervisors typically accept the value of such programmes but challenges can arise around regulatory expectations such as from the draft Guidelines on outsourcing to cloud service providers if the principle of proportionality is not applied. We would urge EIOPA to consider clarifying its expectations where jurisdictional supervisory bodies have not implemented 'regulatory sandbox' regimes in support of industry agile innovation labs. From an Irish Life perspective, we take a tiered approach, with Tier1 being the most important and Tier 4 being the least important. There are two main drivers we consider when weighting for proportionality: - The presence of personally identifiable information (PII) - Risk-prioritised resiliency requirements The above are broadly driven by the potential negative consequence should some adverse event occur. As a Tier 1 example relating to personally identifiable information (PII), in the event that a cloud implementation involves storage of large volumes of PII, or special categories of personal data regarding customers pensions (health data), we are most concerned about the potential impact of a fine under the General Data Protection Regulations (GDPR). However, as an alternate Tier 3 example, we would be less concerned about an online training system where only an employee's name and email address might be captured. It should be noted that per our risk operating model, in the above examples the same level of due diligence would be carried out by ISO & Privacy units within our business. Further, we also engage with suppliers that we weight as Tier 4 contracts; these typically do not include PII and/or do not require a high level of	

Response to the public consultation question	EIOPA Comments
resilience. With that in mind, the level of due diligence carried out is minimal, as is proportional to the risk. When assessing third party arrangements which are not held with cloud service providers but which rely significantly on cloud infrastructure, then the principle of materiality and proportionality will be key. Otherwise, the regulatory cost of implementing the Guidelines will far outweigh any benefit to the undertaking.	
2. Is the set of definitions provided appropriate and sufficiently clear?	
No, see document attached.	Please see the EIOPA comments to the concerns raised by the respondent at Question 1.
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?	
It depends on whether proportionality and materiality in assessment of the cloud services providers applies. Also depends on whether it is assumed that prima facie if something is in the cloud it is automatically deemed outsourcing.	**EIOPA noted the concerns raised by the respondent**
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, see document attached. **Excerpt from Irish Life Group's document** Guideline 1 Irish Life Group disagrees with the assumption that an arrangement with a cloud service provider should prima facie be deemed outsourcing. It is unclear why cloud service providers should be singled out for this specific assumption. In common with other EBA definitions and MiFID II Guideline definitions of outsourcing hinge on an arrangement where the "service provider performs a process, a service or an activity that would otherwise be undertaken by the institution itself". In many instances cloud services are used to carry out activities that an insurance undertaking would never be doing itself. For example, an insurer would not typically be in the business of developing its own software and as a result may well often source software externally, with SaaS arrangements being one option. In addition, what constitutes "an activity that would otherwise be undertaken" by a typical insurance undertaking will change over time in accordance with new market norms and the evolution of business models. Thus the internal definition of what constitutes 'outsourcing' for an undertaking may be expected to change over time. This will create scope for confusion and potential for inappropriate levels of applied governance over certain suppliers should the Guideline deem all cloud service providers to be prima facie cases of outsourcing. It is a significant assumption to indicate that "as a rule, outsourcing should be assumed". Designation as 'outsourcing' has significant implications under Solvency II, not least because in EIOPA Explanatory Text supporting its Guidelines on System of Governance indicates that "in determining whether	**EIOPA partially agrees with the concerns raised by the respondent.** The determination of whether (or not) the purchase of cloud services fall into the scope of outsourcing is paramount to a successful and coherent application of these Guidelines. The assessment to this application is responsibility of the undertakings and should be carried out by applying the criteria provided in Guideline 1 and in the regulatory obligations listed in the introduction of these Guidelines. There are two type of arrangements with third parties service providers: 1) Services which are not outsourcing and 2) Services, which are outsourcing. Among the services which are outsourcing there is a distinction between: - outsourcing of critical or important operational functions (which includes, but is not limited to, insurance and reinsurance processes and activities, functions as defined by Solvency II art. 13(29), provisioning of on-going day to day systems maintenance or support, investment of assets or portfolio management, etc.) - outsourcing of non-critical, non-important operational functions (i.e. less material). In case of outsourcing, an undertaking has to ensure that it remains fully responsible for discharging all its obligations when outsourcing any function or activities (as stated in EIOPA System of Governance paragraph 1.14). For the outsourcing of critical or important operational functions or activities, an undertaking must meet certain requirements.

Response to the public consultation question	EIOPA Comments
an outsourced function or activity is critical or important the undertaking has to take into account any definition or list of such functions or activities provided under national law or national administrative interpretation". Such definitions and lists may not always be pre-fixed with the notion of proportionality or a notion of proportionality that is consistent with that espoused by EIOPA's own Guidelines. As an example, in EIOPA Explanatory Text supporting its Guidelines on System of Governance 'provision of data storage' is stated as an example of a critical or important function. Dependent on the interpretation of the specific activities that constitute data storage this could lead to cloud suppliers "as a rule" being deemed to be outsourcing, and by definition of their data support structures, also 'critical or important'. This could lead to disproportionate and inconsistent levels of governance across members states compared to the risk if proportionality in not applied in relation to such things as the type and volume of the data being stored. Conversely, EIOPA Explanatory Text supporting its Guidelines on System of Governance also indicates that "purchase of standardised services" cannot be considered 'critical or important'. However, background to this consultation states "compared with more traditional forms of outsourcing offering dedicated solutions to clients, cloud outsourcing services are much more standardised, which allows the services to be provided to a larger number of different customers in a much more automated manner and on a larger scale". Clarity is needed on apparently contradictory statements contained in related Guidelines and the interplay between the Guideline and separate definitions or lists of outsourced functions or activities (and their criticality) provided elsewhere under national law or national administrative interpretation.	When an undertaking purchases cloud services, it has to perform the same type of assessment due in case of "general outsourcing", namely 1) understand whether the purchase of cloud services is outsourcing or not; 2) if it classifies as outsourcing, understand whether the outsourced function is critical or important; 3) on critical or important operational functions or activities, perform a detailed risk assessment on the operational function/activity to be outsourced and a detailed due diligence on the service provider; 4) On all the less material outsourcing, in order to fulfil its responsibility obligation (as stated above), a risk assessment and a due diligence (of higher level compared to the previous point) are to be performed. Furthermore, notwithstanding the results of the assessment of whether or not the provisioning of cloud services falls under the definition of "outsourcing", as part of their internal control system, on a risk and proportionate way, the undertaking should identify, measure, monitor, manage and report risks caused by arrangements with third parties regardless whether or not those third parties are cloud service providers. On the respondent request to eliminate the sentence "as a rule outsourcing should be assumed" from the Guideline, in light of the above, EIOPA deleted that sentence. **EIOPA updated the Guidelines accordingly.**
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?	
YES	NA
5b. Is the Guideline on written policy consistent to the market best practices on defining the policy for general outsourcing?	
YES	NA
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?	
This question is more appropriate for national supervisory authorities.	**EIOPA noted the concerns raised by the respondent.**
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?	
Have supplier arrangement processes in place - however it would have a significant impact if prima facie all cloud providers where deemed outsourcing and if proportionality and materiality were not operational. **Excerpt from Irish Life Group's document**	**EIOPA partially agrees with the concerns raised by the respondent.** EIOPA has streamlined the content of the Guideline 5 in order to make it more principle and risk based by removing the requirements for keeping a register

Response to the public consultation question	EIOPA Comments
Guideline 5 Clarity should be provided on whether what is envisaged is one central register or if the location of the data within a series of registers/lists within an undertaking is sufficient i.e. audit dates and next scheduled audits are generally held within the control functions rather than the outsource register.	and requiring the undertaking to record information of their cloud outsourcing arrangements. **EIOPA updated the Guidelines accordingly.**
7b. What can be other approaches to ensure a proper and sound holistic oversight of cloud outsourcing?	
These will need to evolve as the nature of cloud outsourcing changes.	**EIOPA noted the concerns raised by the respondent.**
8. Are the documentation requirements appropriate and sufficiently clear?	
YES	NA
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, see document attached. **Excerpt from Irish Life Group's document** Guideline 7 Guideline 7 states: *"Prior to entering into any outsourcing arrangement with cloud service providers, the undertaking should assess if the cloud outsourcing has to be considered 'material'. The assessment should take into account whether the cloud outsourcing is related to critical or important operational functions as referred to in the Solvency II Directive and in the Delegated Regulation and whether the cloud outsourcing is materially affecting the risk profile of the undertaking. In performing such assessment, where relevant, an undertaking should take into account the possible extension and foreseen changes to the cloud services' scope."* Irish Life would challenge a requirement that the materiality of a cloud service arrangement be determined based on possible extension or extension of the scope of those services. Heightened materiality will impose heightened levels of governance. This should only be required when foreseen changes are 'probable' or being implemented and should then form part of the due diligence carried out at that time. Furthermore it is stated that: *"Moreover, in order to determine the materiality of cloud outsourcing, undertakings should take into account, together with the outcome of the risk assessment, at least the following factors […] the undertaking's aggregated exposure to the same cloud service provider and the potential cumulative impact of outsourcing arrangements in the same undertaking's business area"* Clarity is sought on whether the intent is for an undertaking to consider concentration risk where cloud service providers offer direct services, or whether the intent also for an undertaking to consider concentration risk at a sub-contractor level. Irish Life is of the view that concentration risk should be considered where a cloud service provider is a direct provider of services to	**EIOPA partially agrees with the concerns raised by the respondent.** On the use of the term "material" instead of the term "critical or important", as reported above, bearing in mind that one of the main purposes of these Guidelines is to provide clarity to the market participants, EIOPA decided to withdraw the use of the term "material outsourcing" sticking to the term "critical or important operational function and activity". On the other specific comments, EIOPA: - at paragraph 28 of the Guidelines (former paragraph 25), substituted the word "possible" with the periphrasis "has the potential to become"; - is the opinion that the undertaking should consider the concentration risk also at the level of sub-contractors in case they do critical or important operational functions or activities (for example if the sub-contractor is providing cloud infrastructure for a critical application/system used by the undertaking to perform a critical or important function); - agrees with the respondent that an undertaking should consider its concentration risk within its corporate (or group when applicable) perimeter. With reference to the last points, EIOPA wishes to clarify that having an understanding on whether the cloud service provider has a market dominance could be a useful information that the decision making body should weigh in the risk assessment to decide whether or not outsource to that specific cloud service provider the specific service. The Guidelines do not preclude the outsourcing to cloud service providers with market dominance or that it is not easily substitutable; **EIOPA updated the Guidelines accordingly.**

Response to the public consultation question	EIOPA Comments
the undertaking, however, it may not be possible or feasible to consider concentration risk where the cloud provider is providing services to a third party who in turn provides services to the undertaking. Clarity is also sought on whether the intent is for an undertaking to consider concentration risk within just their own business or also more broadly across their industry area. Irish Life is of the view that concentration risk should be considered within a business, but that it may not be possible or feasible for an individual business to consider concentration risk relating to cloud providers more broadly across the industry. Market concentration risk should be monitored and examined by the national competent authority.	
10. Is the content of Guideline on risk assessment of cloud outsourcing appropriate and sufficiently clear?	
No, see document attached. **Excerpt from Irish Life Group's document** Guideline 8 *"The undertaking should assess the potential impact of material cloud outsourcing both before and after the outsourcing particularly on their operational risk, strategic risk, concentration risk and reputational risk. The assessment should include, where appropriate, scenario analysis of possible but plausible, including high-severity, operational risk events.* *Moreover, within their risk assessment in case of material cloud outsourcing, the undertaking should also take into account the expected benefits and costs of the proposed cloud outsourcing arrangement performing a cost-benefit analysis to be approved, as part of the overall approval, by the AMSB."* Additional clarity is sought around the provision set out above and how the principle of proportionality interplays with the assessment underlined. Supplier risk assessments are often a designated activity / process within organisations. Cost versus benefit analysis typically takes place as part of Business Case development with outputs from the two parallel processes included in any request for Board approval. Strict interpretation of "within their risk assessment" could require amalgamation of parallel processes which is presumably not the intention. In addition, we would question why a number of the provisions within this Guideline are being addressed to cloud services providers given they are not cloud specific requirements.	**EIOPA partially agrees with the concerns raised by the respondent.** EIOPA reviewed extensively the content of Guideline 11 on risk assessment to ensure a better inclusion of the principle of proportionality by: (1) reducing the number of areas to be checked during the risk assessment; (2) enhancing the flexibility of application of the Guideline; (3) focusing the scope of application of the Guideline only on critical or important operational functions and activities outsourced. As a result of the review, the point raised by the respondent has been reviewed. **EIOPA updated the Guidelines accordingly.**
11. Are the contractual requirements for material outsourcing appropriate and sufficiently clear?	
No, see document attached.	**NA**

Response to the public consultation question	EIOPA Comments
12. Are the criteria provided to set the contractual requirements for non-material outsourcing appropriate and sufficiently clear?	
No, While the criteria and Guidelines are generally appropriate and sufficiently clear, some further consideration should be given to the risk proportionality drivers highlighted in our response (data classification, volumes of data, and resilience). **Excerpt from Irish Life Group's document** Guideline 11 *"The outsourcing agreement should not limit the undertaking's information, access and audit rights as well as control options on cloud services in order to fulfil all its regulatory obligations. Additionally, it should be ensured that the undertaking receives the information it needs to adequately manage and monitor the risks associated with cloud outsourcing arrangements."* Irish Life would like clarification of the extent to which an undertaking's requirements for information, access and audit rights as well as control options on cloud services can be tailored to the risk profile of the service and provider in question. Our view is that the extent to which information, access and audit rights as well as control options on cloud services are available need only be sufficient to adequately manage and monitor the risks associated with cloud outsourcing arrangements. As examples: - The right to audit may not be necessary where the provider is an industry standard provider and makes an appropriate assurance report available to their customers; - The ability to configure controls depends on the nature of the service and the provider. Many of the configuration settings are defined by the service provider for PAAS or SAAS solutions. An appropriate assurance report may provide comfort that these are appropriate. *"…. Undertakings may use….third party certifications and third-party or internal audit reports made available by the cloud service provider; pooled audits (i.e. performed jointly with other clients of the same cloud service provider), audit performed by third clients or by a third party appointed by them. .. 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."* Irish Life would like clarification on the expectation of having a 'contractual right to request the expansion of the scope'. Generally the content of assurance reports or third party certification should be considered as part of due diligence process to ensure it provides appropriate coverage. In normal circumstances an undertaking can request a change to the scope of the assurance report or certification (as with any service). This can be done at the	**EIOPA partially agrees with the concerns raised by the respondent.** EIOPA clarified the scope of application of the Guideline 11, which will be applicable only in case of cloud outsourcing of critical or important operational functions or activities. Furthermore, in order to foster the development of European-wide standards in the area of auditing cloud services for financial institutions, EIOPA aligned the conditions to use third party certifications or audit reports to the ones set by the EBA Guidelines on outsourcing (paragraphs 92-93). These conditions include, in case of outsourcing of critical or important operational functions or activities to cloud service providers, the requirement for the undertakings to not rely solely on third-party certifications and reports over time. This means that undertakings should not simply assume that receiving a certificate or a report is enough assurance that the cloud service is being provided in accordance with their legal, regulatory and risk management obligations. If an undertaking elects to use third party certifications as audit tool, such undertaking should assess the adequacy of the information in these certifications against its own requirements and make follow-up enquiries to the cloud service providers if necessary (which might include the performance of on-site audits or require the provider to expand the scope of the certification or of the audit report in the next version of the certification or of the audit report). **EIOPA updated the Guidelines accordingly.**

Response to the public consultation question	EIOPA Comments
point of engaging with the vendor or if this is required due to a change in services or processes. However, the right to request is generally not enshrined within a contract in the Irish market.	
13. Are the Guideline on access and audit rights appropriate and sufficiently clear	
14. Are the provisions set by this Guideline for security of data and systems appropriate and sufficiently clear?	
While the criteria and Guidelines are generally appropriate and sufficiently clear, some further consideration should be given to the risk proportionality drivers highlighted in our response (data classification, volumes of data, and resilience). **Excerpt from Irish Life Group's document** Guideline 12 *For the purposes of the previous paragraph, an undertaking, prior to outsource to cloud service providers, on the basis of the results of the risk assessment performed in accordance with Guideline 8, should …….. monitor the level of fulfilment of the requirements relating to the efficiency of control mechanisms implemented by the cloud service provider and its significant sub-outsourcers that would mitigate the risks related to the provided services."* Irish Life would like clarification relating to the nature and extent of monitoring that would be expected to be carried out. A 'one size fits all' approach taken to all outsourcing would be difficult and time consuming to complete. Additional guidance relating to prioritisation based on risk would be beneficial. It may be further worth clarifying if the engagement of service auditors or reliance on 3rd party certifications as highlighted in Guideline 11 would be sufficient to address the intent of this monitoring.	**EIOPA agrees with the concerns raised by the respondent** A 'one-size fits all' approach is likely not working when monitoring operational functions or activities outsourced to cloud service providers. The level and the type of monitoring mechanisms that an undertaking should set up should be defined bearing in mind the nature, scale and complexity of the inherent risks in the services outsourced to cloud service providers. This monitoring mechanisms might include third parties certifications. **EIOPA updated the Guidelines accordingly**
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, while the criteria and Guidelines are generally appropriate and sufficiently clear, some further consideration should be given to the risk proportionality drivers highlighted in our response (data classification, volumes of data, and resilience). **Excerpt from Irish Life Group's document** Guideline 13 *"To comply with the requirements of Article 274(4)(k) and (l) of the Delegated Regulation, the cloud outsourcing agreement should specify, where relevant, whether or not sub-outsourcing of critical or important functions or activities of the undertaking, or significant parts thereof, are permitted or expressly excluded. The undertaking should agree to sub-outsource only if the sub-*	**EIOPA partially agrees with the concerns raised by the respondent** On Guideline 13 (sub-outsourcing), EIOPA changed the title of the Guideline to "Sub-outsourcing of critical of important operational functions or activities" and clarified its contents. **EIOPA updated the Guidelines accordingly**

Response to the public consultation question	EIOPA Comments
outsourcer will also fully comply with the obligations existing between the undertaking and the cloud service provider. These obligations include the audit and access rights and the security of data and systems as defined by the Solvency II Directive and the Delegated Regulation and further specified by these Guidelines." It is the view of Irish Life that the scope of this Guideline should be reduced to apply only to relevant contractual obligations and allow for reliance to be placed on third party contractual provisions.	
16. Do you have any comments on the impact assessment?	
We do not disagree with the explanatory commentary but we do disagree with the prima facie assumption of all cloud arrangements being deemed outsourcing. Please see document attach **Excerpt from Irish Life Group's document** Conclusion The nature and scale of services that can now be accessed via cloud services providers is constantly increasing and will continue to do so for the foreseeable future. In addition, cloud service providers hold very technical experience on a number of areas including security benefits which are core to their business. Irish Life Group welcomes the publication of the Guidelines by EIOPA but would stress as stated above the need to ensure proportionality and materiality when putting in place new Guidance. Irish Life would like to note that its experience, albeit that the Irish Life Group is the largest financial services group in Ireland have found the negotiation of changes to standard contractual terms and conditions with cloud services providers exceptionally difficult. The expectation therefore that insurance undertakings of all sizes and scale will be able to negotiate changes to align with these Guidelines is questionable.	**EIOPA noted the concerns of the respondent.** As reported above (Question4), on the respondent request to eliminate the sentence "as a rule outsourcing should be assumed" from the Guideline, in light of the above, EIOPA deleted that sentence
Annex Y/N	
YES	

Cloud service providers

Google Cloud, Ireland

Response to the public consultation question	EIOPA Comments
1. Is the scope of application provided appropriate and sufficiently clear?	
YES	NA
2. Is the set of definitions provided appropriate and sufficiently clear?	
We believe that the definitions of sub-outsourcers, as well as the definitions referring to data policy need clarification as specified in our attached detailed response	**EIOPA noted the concerns raised by the respondent.**
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?	
YES	**EIOPA noted the concerns raised by the respondent.**
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?	
The Guidelines require that authorities and undertakings start from the assumption that all arrangements with cloud service providers are "outsourcing". It is unclear why arrangements with cloud service providers should be treated differently to arrangements with other types of providers. Whether an arrangement amounts to "outsourcing" should depend on whether the definition is met, without an assumption either way. An assumption that arrangements with cloud services providers are "outsourcing" will likely lead to more determinations that these arrangements are "outsourcing". This would be disproportionate if those arrangements do not in fact fall within the definition of "outsourcing". It would also create inconsistency between the application of these Guidelines and the EBA's Outsourcing Guidelines, which do not contain this assumption.	**EIOPA agrees with the concerns of the respondent and updated the Guidelines accordingly**
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?	
In 16 (d), it is not clear that the reference to "contractual requirements" is a reference to the contractual requirements in Guideline 10. This could lead to undertakings and authorities interpreting this Guideline to go beyond the requirements of Guideline 10. In particular, there is a risk that this Guideline could be interpreted as requiring the undertaking to include precise contractual language in their outsourcing policy. Specifying contractual language in the outsourcing policy could: - bring the contract in scope of due diligence before the undertaking and the cloud service provider have a meaningful opportunity to discuss and adjust the terms; and	**EIOPA agrees with the concerns of the respondent and updated the Guidelines accordingly**

Response to the public consultation question	EIOPA Comments
- decrease the undertaking's ability to adapt the contractual requirements to the specific arrangement in question. This could lead to divergent practices by undertakings and authorities because of the potential for different interpretations. If interpreted to require the outsourcing policy contain specific contractual language, this Guideline could lead to: - Cloud arrangements could be summarily disqualified during due diligence in scenarios where perceived gaps could have been addressed in negotiation; - overall contracts for arrangements with cloud service providers could be less fit-for-purpose.	
5b. Is the Guideline on written policy consistent to the market best practices on defining the policy for general outsourcing ?	
See above	NA
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?	
With regards to the requirement for notification of data location, as drafted, the reference to locations where data are "processed" will be problematic if the word "processed" in the Guidelines is given the same meaning as it is under the GDPR. "Process" is defined widely in the GDPR. It would include data transport / transit. Specifying the countries / regions through which data transit would be a challenge because – depending on how the undertaking uses the services – data may (1) transit across networks covering much of the globe, and (2) transit across that global network infrastructure via many different routes. It would be very impractical for undertakings to document the countries/regions through which data transit. A requirement to do this would be disproportionate given the lower risks associated with data in transit versus data at rest. This requirement would also be inconsistent with the approach taken to data in transit under the GDPR in the context of international transfers. Without clarification, this Guideline could also lead to authorities taking different interpretations.	**EIOPA partially agrees with the concerns raised by the respondent.** EIOPA reviewed and streamlined the content of Guideline 4 striving to further align its text to requirements set by the EBA Guidelines on outsourcing. As a result, the change requested by the stakeholder has been included in the Guideline. **EIOPA updated the Guidelines accordingly.**
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	**EIOPA noted the concerns raised by the respondent.**

Response to the public consultation question	EIOPA Comments
7b. What can be other approaches to ensure a proper and sound holistic oversight of cloud outsourcing?	
NO COMMENT	NA
8. Are the documentation requirements appropriate and sufficiently clear?	
The approach to defining the requirements on documenting and providing notifications on data location in the current definitions would be problematic as described above; the approach to defining significant sub-outsourcers also needs clarification. We would also welcome a clarification that the reference to identifying and assessing "all relevant risks" in 24 (b) is a reference to the risk assessment in Guideline 8. Otherwise it could lead to undertakings and authorities interpreting this Guideline to go beyond the assessment in Guideline 8. If so, it will be challenging for undertakings to assess what "all relevant risks" means. We are providing more specific suggestions in the attached detailed response.	**EIOPA noted the concerns raised by the respondent.** EIOPA has streamlined the content of the Guideline 5 in order to make it more principle and risk based by removing the requirements for keeping a register and requiring the undertaking to record information of their cloud outsourcing arrangements. Furthermore, EIOPA has defined, as minimum requirement, a set information to be recorded only for critical or important operational functions outsourced to cloud service providers. This set of information is aligned to the one required by the EBA Guidelines on Outsourcing. As a result, the changes requested by the stakeholder have been included in the Guideline.
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?	
YES	NA
10. Is the content of Guideline on risk assessment of cloud outsourcing appropriate and sufficiently clear?	
We would welcome clarifications on the requirements to data storage and processing in 30 (f), and transfers of personal data in accordance with the GDPR requirements - in 30 (g. i). We are providing more specific suggestions in the attached detailed response.	**EIOPA noted the concerns raised by the respondent.** EIOPA reviewed extensively the content of this Guideline by: (1) reducing the number of areas to be checked during the risk assessment; (2) enhancing the flexibility of application of the Guideline; (3) focusing the scope of application of the Guideline only on critical or important operational functions and activities outsourced. On the specific requests to amend elements of the Guidelines, EIOPA: - simplified the wording of former paragraph 30(f) which has been incorporated into paragraph 31(b-iii); - kept the wording of former paragraph 30(g i) to be consistent with the wording used by the EBA in its Guidelines on outsourcing.
11. Are the contractual requirements for material outsourcing appropriate and sufficiently clear?	
In 35 (g), It is not clear what is meant by "kept" and how this is different to "storing". We understand "store" and "keep" to mean the same thing. Using two different terms would suggest they have different meanings. If so, it is unclear what the difference is. Elsewhere the Guidelines only refer to where data is "stored". This could create uncertainty for both undertakings and cloud service providers. Without clarification, this Guideline could also lead to authorities taking different interpretations.	**EIOPA partially agrees with the concerns raised by the respondent.** EIOPA reviewed extensively the text of the Guideline 10 to ensure a better inclusion of the principle of proportionality. In light of this, EIOPA: (1) reviewed the scope of application of the Guideline which will be applicable only in case of cloud outsourcing of critical or important operational functions or activities;

Response to the public consultation question	EIOPA Comments
In addition, please see our comments on paragraph 18(f) about the reference to "processed". In 36, it is not clear what extra steps an undertaking would need to take in order to take 'special care'. All the requirements of Article 274 of the Delegated Regulation are binding on undertakings. The Guidelines should not create a hierarchy of importance between different requirements in certain contexts. The Guidelines already refer to the principle of proportionality. This aims at ensuring that governance arrangements are consistent with the nature, scale and complexity of the risks. This could create uncertainty for both undertakings and cloud service providers. Without clarification, this Guideline could also lead to authorities taking different interpretations. We are providing more specific suggestions in the attached detailed response.	(2) clarified the relationship between this Guideline and the requirements set by Directive 2009/138/EC and Commission Delegated Regulation (EU) No 2015/35 by eliminating the former paragraphs 36, 37 and 38. Furthermore, bearing in mind the possible complexities of its implementation in case of misalignments between the content of this Guideline and of the one set by the EBA on the same subject, EIOPA further aligned the wording of this Guideline to the EBA requirements set by paragraph 75 of the EBA Guidelines on outsourcing. In light of this, on the specific requests to amend elements of the Guidelines, EIOPA: - substituted the word "kept" with the word "stored" at paragraph 37(f) (former paragraph 35(g)); - kept the wording of former paragraph 35(f) to be consistent with the wording used by the EBA in its Guidelines on outsourcing; - deleted the former paragraph 36. **EIOPA updated the Guidelines accordingly.**
12. Are the criteria provided to set the contractual requirements for non-material outsourcing appropriate and sufficiently clear?	
YES	NA
13. Are the Guideline on access and audit rights appropriate and sufficiently clear	
We would suggest certain amendments to Guideline 11 on access and audit rights to further focus on the effectiveness of audit and access rights. This is consistent with Article 38(1) of the Solvency II Directive, Article 274(4)(h) of the Delegated Regulation, and the EBA approach. The Guidelines could also provide further clarity on important procedural steps such as notice for an on-site visit. Approach to third-party certifications and audit reports also needs to be revised in accordance with the international best practices to ensure that they can provide important information and assurance to customers in a scalable and standardised way. We are suggesting specific amendments in our attached detailed response.	**EIOPA partially agrees with the concerns raised by the respondent.** In order to foster the development of European-wide standards in the area of auditing cloud services for financial institutions, EIOPA aligned the conditions to use third party certifications or audit reports to the ones set by the EBA Guidelines on outsourcing (paragraphs 92-93). These conditions include, in case of outsourcing of critical or important operational functions or activities to cloud service providers, the requirement for the undertakings to not rely solely on third-party certifications and reports over time. This means that undertakings should not simply assume that receiving a certificate or a report is enough assurance that the cloud service is being provided in accordance with their legal, regulatory and risk management obligations. If an undertaking elects to use third party certifications as audit tool, such undertaking should assess the adequacy of the information in these certifications against its own requirements and make follow-up enquiries to the cloud service providers if necessary (which might include the performance of on-site audits or require the provider to expand the scope of the certification or of the audit report in the next version of the certification or of the audit report). **EIOPA updated the Guidelines accordingly.**

Response to the public consultation question	EIOPA Comments
14. Are the provisions set by this Guideline for security of data and systems appropriate and sufficiently clear?	
In 50 (f), it is not appropriate to require undertakings to agree a data residency policy with their cloud service providers in every case regardless of (a) whether it is an appropriate solution to the identified risks, or (b) whether in any event all relevant parties have effective access to data. In addition, please see our comments on paragraph 18(f) about the reference to "processed" above and in the attached detailed response. Addressing risk By requiring a data residency policy in all cases, this Guideline assumes that locating (or not locating) data in select countries will be a proportionate approach in all cases. This may not be true in all cases. For instance, if risks are identified with a particular location, another viable option would be to address those risks using robust technical and governance measures. These can prove to be more reliable in addressing risk than a policy of locating data in certain countries but not others. The EBA Outsourcing Guidelines recognise this. The EBA Outsourcing Guidelines do not mandate a data residency policy in every case. Instead, they require institutions to adopt a risk-based approach to data storage and data processing location(s) and information security considerations (para 83). In addition, any requirement to agree a data residency policy should recognise the undertaking's role in determining where the undertaking's data is stored etc. on a cloud service. Cloud services typically provide customers with location options. If an undertaking agrees a data residency policy with a cloud service provider, but the undertaking's personnel select a location that is not covered by the policy, then this is the undertaking's responsibility. Effective access Article 38(1) of the Solvency II Directive and Article 274(4)(h) of the Delegated Regulation require undertakings, their auditors and their supervisory authorities to have effective access to data/information. Given the functionality of cloud services, it is unclear why a data residency policy is required to achieve effective access. Google Cloud's services, for example, enable customers to access their data regardless of where the data are located.	**EIOPA partially agrees with the concerns raised by the respondent and updated the Guidelines accordingly.**

Response to the public consultation question	EIOPA Comments
In addition, as contemplated in Guideline 10 (Contractual requirements) and Guideline 11 (Access and Audit Rights), undertakings, their auditors and their supervisory authorities will have the ability to conduct audits at any of the cloud service provider's premises. The EBA Outsourcing Guidelines do not mandate data location to ensure effective access. Instead, they require institutions to ensure that the outsourcing arrangement does not impede or limit effective access (para 89). Practical challenges A requirement to agree and comply with a data residency policy for every cloud outsourcing will likely lead to a strict requirement that data is located in certain countries. Even if the policy can be updated over time, this approach will significantly limit an undertaking's ability to quickly realize and maximize the benefits (e.g. decreased latency and increased resilience) of a cloud service provider's full infrastructure - at the outset of the arrangement and as the cloud service provider's geographic footprint expands. This is one of the key benefits of cloud services. Limiting it will have a knock-on effect on the service the undertaking can provide to policyholders. Creating this limitation regardless of whether a residency policy would in fact address the identified risk would be disproportionate. Harmonisation Despite pursuing the same supervisory objectives, the EBA Outsourcing Guidelines do not require institutions to agree a data residency policy in all cases. Adopting a different approach in these Guidelines will cause regulatory fragmentation. For organizations subject to both regimes, it may not be possible to wholly segment data / systems subject to one regime and not the other. This would result in all data / systems having to comply with the less flexible standard in these Guidelines. This could create significant additional knock-on overheads and barriers beyond the scope of these Guidelines. In addition, a requirement for a data residency policy overlaps with the requirements for data transfers under the GDPR where personal data are involved. The GDPR does not prohibit data transfers to specific countries. Personal data can be transferred to any country provided that organizations comply with applicable transfer mechanisms. A requirement for a data residency policy goes beyond, and could potentially conflict with, the GDPR.	

Response to the public consultation question	EIOPA Comments
We are suggesting specific amendments in the attached detailed response.	
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.	
Please see our comments to Recommendations 4 and 5 above and in the attached detailed response	**EIOPA noted the concerns raised by the respondent.**
16. Do you have any comments on the impact assessment?	
NO COMMENT	NA
Annex Y/N	
YES	

Other stakeholders

Pinsent Masons, Legal Firm, United Kingdom

Response to the public consultation question	EIOPA Comments
1. Is the scope of application provided appropriate and sufficiently clear?	
No comment	NA
2. Is the set of definitions provided appropriate and sufficiently clear?	
We are concerned that the definition provide for a cloud broker is a concept specific to these EIOPA Guidelines and not one that is commonly used by financial institutions or technology providers. It is also a concept that is not provided for in the EBA Guidelines on outsourcing arrangements (EBA/GL/2019/02) ("EBA Guidelines"). It is not clear what the rationale is for extending these Guidelines to cloud brokers where they are not also performing outsourcing services as cloud service providers. To the extent that they are cloud service providers they will be covered by the definition of a cloud service provider. To the extent that they are not cloud service providers it is unclear why these arrangements should be covered by the outsourcing provisions of Directive 2009/138/EC ("Solvency II"). We suggest that the definition either be removed or further clarification be given as to the types of arrangements that would fall within the scope of the Solvency II outsourcing provisions which are intended to be covered by this definition.	**EIOPA agrees with the concerns raised by the respondent** In particular, as the concept of cloud broker is not used in the Guidelines, EIOPA decided to delete the definition. **EIOPA updated the Guidelines accordingly.**
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 comment	NA
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?	
We have two key concerns with the approach taken. (1) The EIOPA Guidelines state that "As a rule, outsourcing should be assumed." We think that these words should be deleted. In our view, a more proportionate risk-based approach would be to set out that whether an arrangement is an outsourcing should be assessed objectively on the basis of the tests provided in Guideline 1. Taking this approach would be more consistent with the approach that financial institutions subject to the EBA Guidelines are required to take as the EBA Guidelines do not require businesses subject to those requirements to assume all third party arrangements to be outsourcings. Consistency across both sets of Guidelines will result in greater harmonisation and potentially significant cost reduction benefits through standardisation of risk management processes across the financial sector.	**EIOPA agrees with the concerns raised by the respondent** On the respondent request to eliminate the sentence "as a rule outsourcing should be assumed" from the Guideline, in light of the above, EIOPA deleted that sentence. On the respondent request to include examples if cloud services falling outside the scope of outsourcing, considering that some examples have already been included in the explanatory text of the EIOPA Guidelines on system of governance, EIOPA has decided to not include in the Guidelines examples of cloud services that are not to be considered as outsourcing **EIOPA updated the Guidelines accordingly.**

(2) The EIOPA Guidelines do not contain a list of examples of arrangements that fall outside the definition of outsourcing. The EBA Guidelines sets out a detailed list. We think that a list should be included which is consistent with the list set out in the EBA Guidelines. As the test set out in Guideline 1 for determining whether a cloud arrangement is outsourcing is broad, a list of examples will be helpful from a practical perspective in applying the criteria to particular use cases.	
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?	
Guideline 3, paragraph 16(d) provides that 'contractual requirements for material and non-material cloud outsourcing arrangements' are to be taken into account in updating an undertaking's overarching written outsourcing policy. While we agree that contractual requirements should be taken into account, there is a risk that this Guideline may be interpreted as requiring that the outsourcing policy set out these contractual requirements in detail. Requiring this level of detail would be onerous and may be contrary to the purpose of maintaining an overarching business-wide outsourcing policy. We suggest that paragraph 16(d) be clarified to provide that the policy should make reference to the contractual requirements provided for in the Guidelines generally, but need not set out those requirements in detail in the policy.	**EIOPA agrees with the concerns of the respondent and updated the Guidelines accordingly**
5b. Is the Guideline on written policy consistent to the market best practices on defining the policy for general outsourcing ?	
NO	**EIOPA noted the concerns raised by the respondent.**
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?	
Guideline 4 should clarify the extent to which commercially sensitive information may be redacted.	**EIOPA noted the concerns raised by the respondent.**
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?	
NO COMMENT	NA
7b. What can be other approaches to ensure a proper and sound holistic oversight of cloud outsourcing?	
NO COMMENT	NA
8. Are the documentation requirements appropriate and sufficiently clear?	
In a cloud context data may transit through a number of locations when services are provided. We suggest that Guideline 5, paragraph 23(h) clarify the meaning of 'where the service will be performed', and exclude from that meaning locations where data is merely in transit.	**EIOPA partially agrees with the concerns raised by the respondent.** EIOPA reviewed and streamlined the content of Guideline 4 striving to further align its text to requirements set by the EBA Guidelines on outsourcing. As a result, the change requested by the stakeholder has been included in the Guideline. **EIOPA updated the Guidelines accordingly**
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?	

The way the term 'materiality' has been used in the Guidelines creates confusion and is potentially inconsistent with Article 49 of Directive 2009/138/EC. Guideline 7, paragraph25 asks undertakings to make two assessments – one, whether the cloud outsourcing relates to a critical or important operational function; and two, whether the cloud outsourcing materially affects the risk profile of the undertaking. Article 49 however, is wholly concerned with outsourcing arrangements which relate to critical or important functions and the concept of materiality is relevant in assessing whether an outsourcing of a critical or important function materially impairs the quality of the system of governance of the undertaking. We think that to achieve a more consistent approach with Solvency II, the Guidelines should require undertakings to make an assessment of whether the outsourcing arrangement relates to a critical or important function only and not separately assess whether it materially affects the risk profile of the undertaking. If EIOPA are to retain the approach of additionally asking undertakings to assess whether the cloud outsourcing materially affects their risk profiles, the Guidelines will need to clarify which rules apply to the undertaking if the assessment reveals that an arrangement does not relate to a critical or important function but does materially affect the risk profile of an undertaking. Separate lists which specify which Guidelines apply to which category of agreements would provide greater clarity.	**EIOPA agrees with the concerns raised by the respondent.** In the process of developing the draft version of the Guidelines issued for public consultation, EIOPA opted for the definition of "material outsourcing" with the aim to have a more risk-based approach in the assessment of cloud outsourcing contracts taking into account the specificities of these type of services. EIOPA was aware of the risks of potential confusion between the new term and the well-established concept of "critical or important operational functions or activities" and for this reason, EIOPA asked a specific question in the consultation paper on this point. On the basis of the feedback received and bearing in mind that one of the main purposes of these Guidelines is to provide clarity to the market participants, EIOPA decided to withdraw the use of the term "material outsourcing" sticking to the term "critical or important operational function and activity". For this reason EIOPA changed the title of the Guideline from "Materiality assessment" to "Assessment of critical or important operational functions and activities." **EIOPA updated the Guidelines accordingly**
10. Is the content of Guideline on risk assessment of cloud outsourcing appropriate and sufficiently clear?	
NO COMMENT	NA
11. Are the contractual requirements for material outsourcing appropriate and sufficiently clear?	
The contractual requirements should be directed at written agreements that are deemed to relate to critical and important functions, not those that are 'material'. This would be more consistent with the approach taken in Solvency II. - Guideline 10, paragraph 35(g) refers to the location of where data are 'kept'. For consistency, we suggest that the term 'stored' is used in place of 'kept'. - Guideline 10, paragraph 35(j) provides that service levels should be 'directly measurable'. We are unclear as to how an undertaking can demonstrate that it is 'directly' measuring agreed service levels. We suggest that the word 'directly' be deleted - Guideline 10 paragraph 36 requires undertakings to 'take special care' in relation to audit, access, termination and exit rights. In a contractual context a requirement to 'take special care' is extremely uncertain (we appreciate that this wording has been carried over from the 2006 CEBS outsourcing guidance). We suggest that the reference to taking special care	**EIOPA agrees with the concerns raised by the respondent.** Bearing in mind the possible complexities of its implementation in case of misalignments between the content of this Guideline and of the one set by the EBA on the same subject, EIOPA further aligned the wording of this Guideline to the EBA requirements set by paragraph 75 of the EBA Guidelines on outsourcing. In light of this, on the specific requests to amend elements of the Guidelines, EIOPA: - substituted the word "kept" with the word "stored" at paragraph 37(f) (former paragraph 35(g)); - changed the wording of paragraph 37(i) (former paragraph 35(j)). As a result the words "directly measurable" has been deleted; - deleted the former paragraph 36. **EIOPA updated the Guidelines accordingly.**

be deleted and that the Guideline clarify that undertakings must meet the contractual requirements of Solvency II rather than 'take special care'.	
12. Are the criteria provided to set the contractual requirements for non-material outsourcing appropriate and sufficiently clear?	
NO COMMENT	NA
13. Are the Guideline on access and audit rights appropriate and sufficiently clear	
It is not clear from Guideline 11 whether all paragraphs need be complied with for every outsourcing agreement or only those that relate to critical or important functions. We suggest that Guideline 11 be clarified so that it relates only to agreements for critical or important functions.	**EIOPA agrees with the concerns raised by the respondent.** EIOPA clarified the scope of application of the Guideline, which will be applicable only in case of cloud outsourcing of critical or important operational functions or activities. **EIOPA updated the Guidelines accordingly.**
14. Are the provisions set by this Guideline for security of data and systems appropriate and sufficiently clear?	
We see no rationale as to why EIOPA should impose a requirement for undertakings to agree a data residency policy with cloud providers. This goes above and beyond the requirements of data protection laws and is inconsistent with the approach taken in the EBA Guidelines. If an undertaking has taken steps to ensure that it is complying with data protection laws, the additional layer of a data residency policy is not needed. We suggest that Guideline 12, paragraph 50(f) be deleted.	**EIOPA partially agrees with the concerns raised by the respondent.** Bearing in mind the objectives of these Guidelines and striving to further align the text to requirements set by paragraph 84 of the EBA Guidelines on outsourcing, the reference to the definition of a data residency policy has been removed and substituted with a more principle based instruction. **EIOPA updated the Guidelines accordingly.**
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.	
We note that there is not a question which covers Guidelines 13 to 16 and therefore highlight our concerns in relation to these Guidelines in response to this question. Guideline 13, paragraph 52 should be amended so that sub-outsourcers are required to fully comply with the 'relevant' obligations existing between the undertaking and the cloud service provider and not all obligations. Guideline 15, paragraph 60(a) provides that undertakings should develop exit plans that are sufficiently tested. To reduce uncertainty and inconsistent approaches developing, we suggest that EIOPA provide further guidance on what a sufficient test of an exit plan will involve. For example, the EBA Guidelines provide that a test could involve carrying out an analysis of the potential costs, impacts, resources and timing implications of transferring an outsourced service.	**EIOPA agrees with the concerns raised by the respondent.** On Guideline 13 (sub-outsourcing), EIOPA changed the title of the Guideline to "Sub-outsourcing of critical of important operational functions or activities" and clarified its contents. As a result of the review of the Guideline, the former paragraph 52 has been deleted. On Guideline 15 (Termination rights and exit strategies), EIOPA clarified the meaning of "sufficiently tested" **EIOPA updated the Guidelines accordingly**
16. Do you have any comments on the impact assessment?	
NO	NA
Annex Y/N	
NO	

European Financial Congress, Think-thank, Poland

Response to the public consultation question	EIOPA Comments
1. Is the scope of application provided appropriate and sufficiently clear?	
The scope of application of the Guidelines should be extended to include an additional category of 'insourcing' or an extension of private cloud to cover an insurance group, that is to say, a service model followed by group companies – for this case, the Guidelines should be adjusted accordingly. Additionally, Community Cloud should be reflected in initiatives between specific participants of the insurance market (e.g. in Poland it would be the National Cloud Operator, the Polish Chamber of Insurance or the Insurance Guarantee Fund). Community is not identified unambiguously. The scope of application as well as the legal basis and sources of law in the light of which the Guidelines should be interpreted are clear and exhaustive, referring to both hard law and soft law sources (other related EIOPA Guidelines). With respect to the application of the Guidelines by groups, there are concerns as to the extent to which such provisions are enforceable against non-EU groups which are supervised by local authorities and not an EU-based supervisory authority. For these entities, the Guidelines should limit the applicability of the principle of proportionality (whose correct application is examined by an EU-based supervisor) or even turn more towards a rule-based approach. However, in the case of EU entities which are members of non-European groups, the Guidelines should not restrict the autonomy of their respective EU-based supervisory authorities.	**EIOPA noted the concerns raised by the respondent.** On the point related to the definition of community cloud, EIOPA decided not to incorporate the definitions in the Guidelines sticking to the ones set by the EBA to ensure consistency. On the point related to the application of these Guidelines to non-EU insurance groups, these Guidelines are applicable to their European subsidiaries under supervision of European national supervisory authorities.
2. Is the set of definitions provided appropriate and sufficiently clear?	
The issue of definitions is a fundamental weakness of the Guidelines under review. The Guidelines do not define/explain the concept of outsourcing properly, neither do they define what outsourcing to cloud service providers means, using this name to refer to any activity involving the use of the cloud technology. On the other hand, the definition of a service outsourced to cloud service providers should be based primarily on the answer to the question what kind of service is outsourced, instead of defining the problem solely in respect of the technology used. Alternatively, Community Cloud could be used in initiatives between insurance companies or market initiatives undertaken by multiple insurers on the market (pooling), e.g. a sales support product only for Warsaw-based companies,	**EIOPA partially agrees with the concerns raised by the respondent.** Outsourcing is defined at Article 13(28) of the Solvency II Directive. EIOPA's Guidelines on outsourcing to cloud service providers builds on such definition. Initiative such as the one described by the respondent comment are not prohibited by these Guidelines. EIOPA wishes also to clarify that the aim of these Guidelines is to provide principle based instructions to the undertakings on how to decline the outsourcing provisions when they enter (or they evaluate whether to enter) into an outsourcing arrangement with a cloud service provider. The Guidelines do not forbid any type of arrangement. On the definitions:

Response to the public consultation question	EIOPA Comments
motorcycle sales, workshop support etc. The Guidelines do not explicitly prohibit that. The introduction and definition of the conceptual framework deserve credit. The definition of 'Cloud service providers' may give rise to certain concerns, as while it is indicated that 'Cloud service providers' are entities providing cloud services, it is also stated (in the same definition) that service providers which rely significantly on cloud infrastructure to deliver their services are also covered by the Guidelines. It seems that for the sake of being more specific, it could be indicated that such entities are considered as 'Cloud service providers' for the purpose of the Guidelines. The term 'material outsourcing', on the other hand, corresponds to the definition of 'Outsourcing of critical or important functions' (Solvency II, Commission Delegated Regulation 2015/35 of 10 October 2014) and 'outsourcing of insurance or reinsurance activities and management system functions' from the Polish Act on Insurance and Reinsurance Activity. Therefore, it seems that the introduction of 'material outsourcing' as a new term is unnecessary and instead of resulting in understanding, it may lead to more confusion and interpretation difficulties at the company data level (especially for individuals who do not deal with 'regulated' outsourcing on a daily basis). Definitions of the private, public, community and hybrid clouds refer to an undefined term 'cloud infrastructure' (instead of the defined concept of 'cloud services'), which may raise interpretation concerns. Furthermore: **1)** The definition of 'Significant sub-outsourcer' does not provide for the existence of a chain of significant subcontractors (sub-outsourcers). **2)** Instead of the definition of 'Cloud services' in the Guidelines, it would be advisable to use the definition provided in the NIS Directive, in order to avoid situations where a service is understood as a cloud service according to the Guidelines but not according to the NIS Directive (or vice versa). **3)** We suggest the use of the term 'distinct types of cloud infrastructure' in the definition of 'Hybrid cloud'.	Cloud service provider, EIOPA clarified the definition as follow up of the feedback received on the public consultation. Material outsourcing, on the basis of the feedback received and bearing in mind that one of the main purposes of these Guidelines is to provide clarity to the market participants, EIOPA decided to withdraw the use of the term "material outsourcing" sticking to the term "critical or important operational function and activity". The definition has been deleted Public cloud, Private cloud, Hybrid cloud in order to have market consistency the definitions have been kept aligned to the one used in the EBA Guidelines on outsourcing. No changes have been made. Cloud services, in order to have market consistency the definition has been kept aligned to the one used in the EBA Guidelines on outsourcing. No changes have been made. Significant sub outsourcer on the basis of the feedback received and in order to have market consistency the definition has been deleted **EIOPA updated the Guidelines accordingly**
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?	
The answer to this question most likely depends on the individual assessment of the insurance companies covered by this regulation, and in particular on the number and business importance of cloud solutions employed by these	**EIOPA noted the concerns raised by the respondent.**

Response to the public consultation question	EIOPA Comments
insurance companies. If no cloud solutions are currently in use, the proposed timeline does not pose a major challenge to the respondent, because the transition timeline regarding the adjustment to the Guidelines depends on the principal. The timeline may present a higher risk to insurance companies which rely heavily on cloud solutions, in particular with respect to core systems, if their current contracts with outsourcing providers do not meet the requirements of the Guidelines. The proposed content of the Guidelines is relatively difficult to implement if the cloud technology is already used by the insurance company. It will undoubtedly require substantial efforts and necessitate renegotiations of existing contracts with clients. The implementation of the Guidelines for non-core activities may result in the discontinuation of the technology due to considerable administrative restrictions generating a significant cost increase and compliance risks. It seems, however, that since outsourcing to cloud service providers is not a new concept for the Polish financial market (including insurance), and the scope of topics covered by the Guidelines largely overlaps the topics and solutions addressed in the Communication from the Polish Financial Supervision Authority of 23 October 2017 concerning the use of data processing in cloud computing by supervised entities, the timeline for the implementation of the Guidelines should be regarded as appropriate.	As part of the review of the Guidelines on the basis of the feedback to the public consultation, EIOPA streamlined the contents of the Guidelines, mainly focusing on outsourcing of critical or important operational functions or activities to cloud service providers. These changes have been done to emphasize EIOPA willingness to focus on substance over form. More specifically on the timeline, as response to several comments by the stakeholders, EIOPA moved the date of application to 1 January 2021 and prolonged the period for reviewing the existing arrangements to 31 December 2022. Furthermore, clarification on the due date to perform the update (where needed) to the undertaking policies and internal processes in accordance to the Guidelines has been clarified and set to 1 January 2021
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?	
The definition of outsourcing set out in Article 13(28) of the Directive is not in itself clear as it can be literally interpreted to mean that it refers to any type of contract under which a third party performs a process, a service or an activity which would otherwise be performed by the insurance or reinsurance undertaking itself. A similar problem exists in banking regulations. Obviously, such a broad interpretation distorts the sense of outsourcing understood as the transfer of a process to a third party and having it managed in such a way that the insurance company itself does not have any resources left to take the process back immediately. Paragraph 10 in Guideline 1 does not modify the broad scope of the definition in Article 13, and only exacerbates the interpretation problems instead. For instance, it points not only to the permanent nature of outsourcing, but also to situations where despite having been outsourced, an activity can be carried out by the insurance company itself, and therefore its wording in a way challenges the nature of 'pulling out' the process.	**EIOPA noted the concerns raised by the respondent.** On the definition of Function, in order to avoid the possible confusion with Article 13(29) of Solvency II Directive, EIOPA decided to delete the definition. The definition has been deleted. On the respondent request to eliminate the sentence "as a rule outsourcing should be assumed" from the Guideline, EIOPA deleted that sentence. Furthermore, on the respondent request to include examples if cloud services falling outside the scope of outsourcing, considering that some examples have already been included in the explanatory text of the EIOPA Guidelines on system of governance, EIOPA has decided to not include in the Guidelines examples of cloud services that are not to be considered as outsourcing. **EIOPA updated the Guidelines accordingly.**

Response to the public consultation question	EIOPA Comments
A further issue is the term 'function' used in the Guideline, having a certain meaning according to the Solvency II system – which may cause further interpretation problems. It is unclear whether the authors meant function as defined in Article 19(29) or any potential outsourced activity. Solvency II in Article 13(28) defines as outsourcing an arrangement of any form between an insurance company and a service provider, by which that service provider performs a process, a service or an activity, which would otherwise be performed by the insurance company itself. This provision is clear and unambiguous, but please note that a different, lower risk value should be assigned to an outsourcing service provider which is a wholly-owned subsidiary of the insurance company or its group. Importantly, a particularly valuable feature of Guideline 1 is that outsourcing should be assumed whenever an activity is delivered by a third party. Concerns as to the distinction between cloud services defined as outsourcing and those that do not qualify as outsourcing arise in the context of the conclusions presented in the EIOPA Final Report after consultations No. 13/008 concerning the draft Guidelines on the system of management, paragraph 5.174, which provides examples of activities that should be classified as 'critical or important'. It follows from that report that a cloud service, if it involves data storage or has an effect on the performance of IT systems, should be qualified as a critical and important activity, and therefore it is considered as outsourcing if it is carried out by a third party, as it is difficult to imagine a cloud service that would not be related to the above areas. For the sake of clarity of the Guidelines, it would therefore be desirable, as in the case of the EBA Guidelines, to specify a list of activities which institutions should not consider as outsourced activities when they are transferred to third parties.	
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?	
The proposed solutions seem to significantly extend the existing internal outsourcing regulations and reinforce the standards of oversight for outsourced activities. An example of this is the development, aside from emergency plans, of written exit strategies including detailed process timelines, or indication of the need to include outsourcing as an element of the ORSA process – therefore, it will be mandatory even if the insurance company does not consider this risk as significant from the perspective of its operations. This approach gives rise to further difficulties involving the necessary risk quantification in the ORSA process, as it seems that the outsourcing risk qualifies as an operational risk,	**EIOPA partially agrees with the concerns raised by the respondent.** On the respondent comment related to the ORSA process, EIOPA wishes to clarify that the undertakings could make reference to their cloud outsourcing only if such cloud outsourcing is related to critical or important operational functions or activities and if it is relevant according to the risk profile of the undertaking.

Response to the public consultation question	EIOPA Comments
and operational risks are measured in a simplified manner using the standard formula. The assessment of the adequacy of the standard formula in this context will be practically impossible, for instance due to the fact that insurance companies lack data on the materialisation of this type of risk. No minimum management standard for outsourced IT services / outsourced service maturity level has been defined – e.g. CMMI, Cloud Computing Governance (TOGAF, COBIT (or Val IT/Risk IT Scorecard), ITIL, SOA, ISO 38500), the above standards and good practices address the business needs and IT management. For outsourcing and the highly sensitive area of cloud services, the reference to a standard and its adoption into the Guidelines seems to be very appropriate. Furthermore: (1) In paragraph 13, it would be advisable to reflect the risk of unexpected and sudden termination of a contract with a provider; (2) In paragraph 15, the security strategy and operational risk management strategy could be added next to the IT strategy; (3) In paragraph 16 (a), the security function could be included; (4) In paragraph 16 (c), it would be a good idea to make a direct reference to ISO 27017/27018 standards. It would also be appropriate to stress the need to update not only the outsourcing policy but also the security policy – in particular to reflect the 'Shared responsibility model' (where the provider is responsible for cloud security, and the user is responsible for the security of their own cloud resources). This also applies to ensuring that persons responsible for the administration of the contract with the cloud provider and the use of cloud resources and systems (such as IT or security functions) are properly trained and have the appropriate knowledge and competences.	On the points related to the standards and good practices mentioned by the respondents, EIOPA decided not to include them in the Guidelines to be standard neutral. As part of this decision, EIOPA removed the reference to standards and reports previously included in the draft Guidelines. However, EIOPA wishes to specify that in order to evaluate the suitability of the cloud service provider, an undertaking could use certificates based on international standards. These include but are not necessarily limited to International Safety Information Security Standard ISO / IEC 2700X of the International Organization for Standardization, C 5 Requirement Catalogue of the Federal Office for Information Security, Cloud Security Alliance standards and the ones mentioned by the respondent. On the specific comments made by the respondent: - Being the risk of unexpected and sudden termination of a contract with a provider included in operational risks, EIOPA did not include it at paragraph 17 (former paragraph 13); - EIOPA agrees with the respondent and modified paragraph 19 (former paragraph 15) accordingly; - EIOPA agrees with the respondent and modified paragraph 20a (former paragraph 16a) accordingly; - While, in principle, EIOPA would agree with the suggestion of making a reference to ISO/IEC 27017/27018 in the text of the Guidelines, as reported above, to be standard neutral, EIOPA decided not to include such reference in the Guidelines. With reference to the remark related to the possible need to update multiple internal related policies and processes, EIOPA agrees with the suggestion and updated the Guidelines accordingly. **EIOPA updated the Guidelines accordingly.**
5b. Is the Guideline on written policy consistent to the market best practices on defining the policy for general outsourcing ?	
No comment	NA
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?	
The scope of information is very broad. It seems that in view of the technologies used, it may be very difficult or impossible to answer some questions in an unambiguous way, such as the location of specific data. It should be noted here that Guideline 4 does not cover all information submitted to a supervisory	**EIOPA partially agrees with the concerns raised by the respondent.** The content of Guideline 4 which is related only to outsourcing of critical or important operational functions or activities has been streamlined by: (a) removing the requirement to present a draft copy of the outsourcing agreement

Response to the public consultation question	EIOPA Comments
authority, as it does not take into account the information provided as part of ORSA or SFCR reports. The Polish supervisory authority already requires a lot of very detailed information with respect to reporting on outsourcing of critical and important activities, and therefore the scope of reporting set out in Guideline 4 does not seem to introduce a significant change in this respect. In some cases, reporting under subparagraph (e) could prove difficult, as detailed information on corporate structures and groups of companies will not always be readily available, especially in the case of providers which are members of large international groups. In subparagraph (f), the description of provider's activities should be clearly and precisely limited to the area related to the outsourced process only, in order to avoid the need to describe the full range of activities carried out by a potential provider who may operate across multiple industries.	(b) aligning the requirements to the EBA requirements set by paragraph 54 of the EBA Guidelines on outsourcing to ensure market consistency. **EIOPA updated the Guidelines accordingly.**
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?	
In our opinion, the introduction of a register of all outsourcing contracts into the cloud will not have a significant impact on the current practices of undertakings in this area. Institutions keep records of outsourcing contracts in accordance with the Polish laws. While the minimum scope of recorded information is narrower than that prescribed by the Guidelines, supplementing it with the data required by the Guidelines should not pose a major organisational challenge for institutions, as most of the information is collected for the purposes of risk analysis or due diligence of the insourcer. The introduction of a register containing all items specified in the aforementioned Guideline will certainly mean an increased administrative and bureaucratic burden for new market participants with regard to cloud outsourcing contracts. Furthermore, the special treatment afforded to cloud services (regardless of their level of materiality/significance) is not fully clear, especially in relation to outsourcing of other critical and important services. This will undoubtedly significantly compromise the usability and processing flexibility of cloud outsourcing contracts, which could particularly affect services for which there is a particularly urgent demand and/or the actual use of a non-cloud solution is impossible or very difficult. On the other hand, such detailed reporting methods and tools will probably contribute to facilitating and improving the monitoring of the outsourcing process by insurance companies.	**EIOPA noted the concerns raised by the respondent.** EIOPA has streamlined the content of the Guideline 5 in order to make it more principle and risk based by removing the requirements for keeping a register and requiring the undertaking to record information of their cloud outsourcing arrangements.

Response to the public consultation question	EIOPA Comments
The register of outsourcing contracts is already in use, so it will not have a significant impact, provided that the register can still be kept in any format (such as Excel, Access, or other IT tools).	
7b. What can be other approaches to ensure a proper and sound holistic oversight of cloud outsourcing?	
No comment	NA
8. Are the documentation requirements appropriate and sufficiently clear?	
The requirements are clear but too broad (audits, risk assessment, a description of the monitoring of a given service provider). The scope of requirements appears to be formulated in an unambiguous manner. However, coupled with the nature of outsourced and cloud services, it may give rise to interpretation problems. In this context, doubts arise as to the nature of outsourced services – do they include the possibility of using software, technical support for software used or, for example, data storage or calculation capabilities – which of them qualify as outsourcing (outsourced services), what is the nature of risk, how it will be defined and estimated, and how the service itself should be supervised.	**EIOPA noted the concerns raised by the respondent.**
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?	
It is appropriate, but not clear enough. However, the defect does not lie in the Guidelines (which define the concept of 'materiality'), but in the underlying regulations, which define the concept of 'critical or important operational function'. Paragraph 60 (EIOPA Guidelines on System of Governance) is formulated in a way that makes it actually possible to qualify EVERY activity carried out within an undertaking as a critical or important activity. If every activity is (or can be) qualified as 'important', any (however advisable) attempts to use a 'materiality' filter at the level of the Guidelines are therefore doomed to fail. Without any minimum conditions, materiality is rated too high as a parameter to serve as an objective judgment and standard. There is a very high risk that materiality assessments will differ considerably depending on the market player. For example, if we discuss a basic system supporting a critical process for an insurance company, outsourcing to a cloud can be assessed with a low level of materiality, since insurance contracts exist in paper form and it is possible to recreate the process and provide the client with an adequate and timely resolution of the claim – and therefore a basic system that is critical to business continuity becomes an auxiliary system that 'digitises' the workflow. The Guidelines should additionally include a process to update the materiality assessment.	**EIOPA partially agrees with the concerns raised by the respondent.** On the use of the term "material" instead of the term "critical or important", as reported above, bearing in mind that one of the main purposes of these Guidelines is to provide clarity to the market participants, EIOPA decided to withdraw the use of the term "material outsourcing" sticking to the term "critical or important operational function and activity". In the review of the Guidelines, EIOPA streamlined the criteria contained in Guideline 7 striving to further align the factors to be taken into account when performing the assessment described by the Guideline to the ones requested by paragraph 31 of the EBA Guidelines on outsourcing. As a result of this review, some of the criteria previously foreseen by the Guideline were deleted, including the following respondent requests: - Clarification of former paragraph 27(e); - Clarification of former paragraph 27(h); - Deletion of former paragraph 27(f). **EIOPA updated the Guidelines accordingly.**

Response to the public consultation question	EIOPA Comments
Furthermore: 1) Paragraph 27 states that in order to determine the materiality of a service, aside from risk assessment, a range of factors should be included whose examination would constitute risk assessment in itself; 2) Paragraph 27 (e) should be made more specific, for example by replacing the term 'cost of the cloud outsourcing' with 'annual contract value' or a similar term; 3) In paragraph 27 (h), it could be advisable to make a reference to the Data Protection impact assessment process required by the GDPR. 4) The idea of risk insurance (27 (f)) seems to be risky – while it may offer protection against material losses, it could prove detrimental to companies in the long run if business cannot be recovered after prolonged downtime. 5) The process of materiality verification should be carried out at least once a year, and a disaster recovery process should be provided for particularly critical cloud-based business systems/functions in another geography of the same provider, by another provider or, as a last resort, on premise (as briefly specified in paragraphs 27g and h).	
10. Is the content of Guideline on risk assessment of cloud outsourcing appropriate and sufficiently clear?	
The solutions presented do not seem to raise any concerns. Risk assessment considerations are presented in a concise yet complete manner that captures their substance. The risk assessment presented in the Guidelines is embedded in the risk-based approach concept and is conducted in proportion to the size and business scale of an institution. The assessment of the risk of long and complex chains of sub-outsourcers ruling out or reducing the ability to ensure proper oversight of activities seems to be a complex process with an uncertain outcome and therefore this type of risk should be subject to mitigation (approach based on statutory law is preferred).	**EIOPA noted the concerns raised by the respondent.**
11. Are the contractual requirements for material outsourcing appropriate and sufficiently clear?	
The requirements are clear; however, some of them are difficult to meet for objective reasons, such as setting out the location where data will be processed. Given the common use of distributed data centres, a service provider itself may not be aware which 'machine' supports a given entity at a given point in time, and the locations are so plentiful that listing them all would not produce the expected supervisory outcome. It seems that the question should be whether the entity performs the contract in accordance with the agreed rules and the laws applicable to the insurance company, and not where the contract is actually performed. Jurisdiction over the contract itself and over the registered office of the entity is important, and so is the performance security, if any.	**EIOPA noted the concerns raised by the respondent.**

Response to the public consultation question	EIOPA Comments
12. Are the criteria provided to set the contractual requirements for non-material outsourcing appropriate and sufficiently clear?	
These requirements in fact refer to a rather general criterion of the type of data outsourced to a cloud. Perhaps the examples prepared by EIOPA have contributed to a better understanding of what contractual requirements should be included in the contract depending on the data type. On the other hand, it is difficult to imagine that outsourcing contracts involving significant amounts of data, production data or sensitive data would not be considered material/important. In our view, in practice this wording used in the Guideline is likely to mean that insurance companies will need to take a conservative approach and seek/endeavour to include all the requirements of Guideline 10 in their cloud outsourcing contracts, regardless of the materiality level. Furthermore: 1) In paragraph 35, it should be ensured – perhaps by adding more detail to subparagraph (e) – that information on incidents (at least those critical) is provided to the insurance company. The insurance company should also be informed of any planned unavailability. 2) In paragraph 35 (h), it would be useful either to define individual attributes or to refer to attributes defined in ISO2700X or the NIS Directive in order to avoid confusion of terms. 3) In paragraph 35 (m), it would be useful to add the obligation to inform the insurance company about testing results. 4) Paragraph 50 fails to cover several issues which surface as security weaknesses in the practical application of clouds within organisations, due to the inadequacy of policies, technologies and knowledge relevant to on-premise security management. These issues involve: a) Security monitoring relevant to the cloud-based service model b) Understanding of security mechanisms offered by a cloud service provider and their proper application, in particular with regard to secure service setup; c) Definition of security requirements (procedural and architectural) relevant to cloud services and reflecting them in the pre-service on-boarding and validation process; d) Clear separation of responsibilities and a cooperation model in case of actual or suspected security incidents (with predefined response times).	**EIOPA noted the concerns raised by the respondent.** EIOPA reviewed extensively the text of the Guideline to ensure a better inclusion of the principle of proportionality. In light of this, EIOPA: (1) reviewed the scope of application of the Guideline which will be applicable only in case of cloud outsourcing of critical or important operational functions or activities; (2) clarified the relationship between this Guideline and the requirements set by Directive 2009/138/EC and Commission Delegated Regulation (EU) No 2015/35 by eliminating the former paragraphs 36, 37 and 38. Furthermore, bearing in mind the possible complexities of its implementation in case of misalignments between the content of this Guideline and of the one set by the EBA on the same subject, EIOPA further aligned the wording of this Guideline to the EBA requirements set by paragraph 75 of the EBA Guidelines on outsourcing. In light of this, on the specific requests to amend elements of the Guidelines, EIOPA: - deleted the former paragraph 35(e); - kept the wording of former paragraph 35(m). On the comments related to Guideline 12 (Security of data and systems), EIOPA agrees with the respondent. As a general principle, cloud customers (i.e. undertakings) are always responsible for what they do in the cloud and the cloud service providers are responsible for the cloud ('Shared responsibility framework"). In light of this it is paramount to define clear roles and responsibilities and for the undertakings to understand the security mechanisms offered by the cloud. **EIOPA updated the Guidelines accordingly.**

Response to the public consultation question	EIOPA Comments
5) Planning and following a training process to maintain an appropriate level of knowledge (which could be demonstrated by technical certificates).	
13. Are the Guideline on access and audit rights appropriate and sufficiently clear	
It could be difficult for institutions to exercise such broad rights of access and auditing. Auditing of sub-outsourcers could pose a particular challenge, especially in the case of very complex outsourcing chains. Making equipment available to institutions or other designated entities may result in a breach of the supplier's business secrets, or even professional secrecy. It should be assumed that most organisations will not conduct their own provider audits and will instead rely on reports from auditors such as SOC – Service Organization Controls, ISAE3402, etc. It would be appropriate for the Guidelines to include provisions concerning the frequency of obtaining such reports, analysing the auditor's opinion, adjusting the provider's objectives and controls to the organisation's internal control environment and risk management system, analysing the impact of reservations to the auditor's opinion and/or identified exceptions and questions, and ensuring that the user-organisation controls mentioned in the auditor's report have been implemented and are effective. Furthermore: - If SSAE18 is sufficient in respect of meeting the expectations of paragraph 45, it would be useful to state this directly, and otherwise it would be appropriate to indicate what should be added to the report. - Paragraph 46 should indicate what else insurance companies should rely on (even by way of example). We also suggest that audit firms should be rotated (e.g. in a 5-year cycle).	**EIOPA partially agrees with the concerns raised by the respondent.** EIOPA clarified the scope of application of the Guideline, which will be applicable only in case of cloud outsourcing of critical or important operational functions or activities. Furthermore, in order to foster the development of European-wide standards in the area of auditing cloud services for financial institutions, EIOPA aligned the conditions to use third party certifications or audit reports to the ones set by the EBA Guidelines on outsourcing (paragraphs 92-93). These conditions include, in case of outsourcing of critical or important operational functions or activities to cloud service providers, the requirement for the undertakings to not rely solely on third-party certifications and reports over time. This means that undertakings should not simply assume that receiving a certificate or a report is enough assurance that the cloud service is being provided in accordance with their legal, regulatory and risk management obligations. If an undertaking elects to use third party certifications as audit tool, such undertaking should assess the adequacy of the information in these certifications against its own requirements and make follow-up enquiries to the cloud service providers if necessary (which might include the performance of on-site audits). **EIOPA updated the Guidelines accordingly.**
14. Are the provisions set by this Guideline for security of data and systems appropriate and sufficiently clear?	
For many individual insurance companies, Guideline 12 will be in many respects difficult to follow. This applies in particular to the control of actual cloud data management, which requires specialist knowledge and access to the technological solutions of the cloud service provider. The decision to use a cloud is often dictated by insufficient qualified in-house resources to maintain high security standards. In the light of the above, an acceptable solution would be to adopt the same principles as in Guideline 11, i.e. to include certificates and third party audits and to monitor the design of the security management system itself.	**EIOPA partially agrees with the concerns raised by the respondent and updated the Guidelines accordingly**

Response to the public consultation question	EIOPA Comments
Monitoring of provider vulnerability management by insurance companies is not addressed. We also suggest that penetration testing should be referenced directly as the expected approach to verification of the material security level of outsourcing. It would also be appropriate to reflect the 'Shared responsibility model' (where the provider is responsible for cloud security, and the user is responsible for the security of their own cloud resources).	
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.	
The Guidelines do not follow the principle of proportionality, as the proposed outsourcing approach covers all activities of an insurance company, regardless of their materiality. The materiality criteria applied do not relate to the essence of outsourcing, instead they are based on the cost of the contract and the risks generated. Outsourcing is not an end in itself, but an entity's response to its actual capabilities and the risk mitigation method. In addition, a distinction needs to be made between outsourcing and mandate, software purchase, consulting, support or other types of contracts with third parties. Outsourcing means subcontracting an organisation out a process which is not or will not be supported internally, because the Company cannot or does not want to maintain it, perhaps due to significant costs of the process. For instance, outsourcing should not include: using a cloud-based office suite, which is purchased software and, as a rule, is supported by a third party (similarly to a car that is serviced under warranty by an authorised provider but no one would claim that the purchase of a car and its servicing classify as outsourcing, because in theory it could be manufactured and serviced for the organisation on an individual basis, incurring a certain level of expenditure). By analogy, use of database space would not be considered as outsourcing either, as no one regards the manufacture or purchase of portable hard drives on which data resources can be stored as outsourcing. On the other hand, it would be considered as outsourcing if an end-to-end process is transferred to a cloud, such as fully independent management of the system administration process or full assignment of services relating to a specific IT system (from	**EIOPA partially agrees with the concerns raised by the respondent** The determination of whether (or not) the purchase of cloud services fall into the scope of outsourcing is paramount to a successful and coherent application of these Guidelines. The assessment to this application is responsibility of the undertakings and should be carried out by applying the criteria provided in Guideline 1 and in the regulatory obligations listed in the introduction of these Guidelines. There are two type of arrangements with third parties service providers: 1) Services which are not outsourcing (for example, non-recurrent activities – as detailed in Guideline 1 – and purchases of goods – including software licences – are not considered as outsourcing arrangements) and 2) Services, which are outsourcing. Among the services which are outsourcing there is a distinction between: - outsourcing of critical or important operational functions (which includes, but is not limited to, insurance and reinsurance processes and activities, functions as defined by Solvency II art. 13(29), provisioning of on-going day to day systems maintenance or support, investment of assets or portfolio management, etc.) - outsourcing of non-critical, non-important operational functions (i.e. less material). In case of any outsourcing (regardless if it of critical or important operational functions) an undertaking has to ensure that it remains fully responsible for

Response to the public consultation question	EIOPA Comments
development to implementation, administration, to the introduction of production changes for corporate purposes). Further to that, the said definition of outsourcing would not require the assessment of service materiality, as subcontracting out the entire process of company functioning is material by nature. However, the above approach does not hinder the management of the risks arising from external contracts. These risks should be managed (but not as an outsourcing risk), for example data security guaranteed in databases (just like data security on a portable drive), but the nature of the risk is different and it is analysed under a contract. In the first case, data availability, security and integrity are important for the undertaking, while in the second case it is the ability to run a business process in view of a lack of internal resources. Therefore, risk mitigation methods will be different. In the first case, these will be data backups, and in the second case – ensuring a smooth transition between the teams supporting the process (regardless of their location). To sum up, the Guidelines should be preceded by defining exactly when the outsourcing service occurs and, additionally, a separate subset should indicate in which cases a cloud service is an outsourcing service. Furthermore: 1) In paragraph 56 (e), the purpose of distinguishing between IT security and cybersecurity is not clear. Additionally, the expectation for a clear separation of IT and non-IT processes expressed in this section will not always be possible (for example where insurance products are sold by electronic means); 2) In paragraph 60 (a), it is not clear in which cases the testing is actually expected; 3) If operational risk in the insurance sector is to be defined in the same way as it is in the banking sector, then IT risk should be included in the operational risk framework; 4) In addition, we suggest the introduction of a mechanism for cooperation and knowledge sharing between supervisory authorities to ensure a uniform supervisory approach and a level playing field; 5) Paragraph 60 (b) refers to the identification of alternative solutions. For important and critical systems, solutions enabling easy change of provider	discharging all its obligations when outsourcing any function or activities (as stated in EIOPA System of Governance paragraph 1.14). For the outsourcing of critical or important operational functions or activities, an undertaking must meet certain requirements. When an undertaking purchases cloud services, it has to perform the same type of assessment due in case of "general outsourcing", namely 1) understand whether the purchase of cloud services is outsourcing or not; 2) if it classifies as outsourcing, understand whether the outsourced function is critical or important; 3) on critical or important operational functions or activities, perform a detailed risk assessment on the operational function/activity to be outsourced and a detailed due diligence on the service provider; 4) On all the less material outsourcing, in order to fulfil its responsibility obligation (as stated above), a risk assessment and a due diligence (of higher level compared to the previous point) are to be performed. Furthermore, notwithstanding the results of the assessment of whether or not the provisioning of cloud services falls under the definition of "outsourcing", as part of their internal control system, on a risk and proportionate way, the undertaking should identify, measure, monitor, manage and report risks caused by arrangements with third parties regardless whether or not those third parties are cloud service providers. On the points raised by the respondent, EIOPA: - removed the former paragraph 56(e); - clarified the meaning of "sufficiently tested"; - operational risks are defined as in the banking sector, however, given their relative importance in the field of cloud outsourcing, EIOPA decided to highlight ICT risks; - on the mechanisms for cooperation between supervisory authorities, EIOPA included a specific Guidelines on the supervision of cloud outsourcing addressed to supervisory authorities. Furthermore, as part of its role, foster supervisory convergence on this area; - EIOPA agrees with the remark of the respondent on alternative solutions enabling easy change of provider (multi-cloud). Furthermore, EIOPA wishes to mention, in this regard, the initiative to develop a SWIPO code of conduct run by the European Commission. **EIOPA updated the Guidelines accordingly.**

Response to the public consultation question	EIOPA Comments
(multi-cloud), which do not consume significant effort or time, should be preferred instead (to avoid a 'vendor lock').	
16. Do you have any comments on the impact assessment?	
impact assessment is extremely useful as an introductory document. It perfectly shows the alternatives available to the authors of the Guidelines and contributes to understanding why the options which are now the 'backbone' of the document under development have been finally chosen. However, in the impact assessment, EIOPA actually did not describe any quantifiable impacts of the introduction of the Guidelines on insurance activities and the IT services industry. Reference was only made to potential compliance risks due to differing definitions of the same problems by national supervisors. Market benefits, on the other hand, are defined only in the framework of harmonisation of standards. The document does not indicate that the regulation itself would generate transposition costs, as a minimum. Significant regulatory risks which should be mentioned here include inhibiting the development of the cloud technology in the financial sector, as it may turn out too expensive and too risky for insurance companies to implement in their operations. At the same time, the proposed legislative solutions do not address the main problems involved in the business of insurance companies, including personal data protection, limited highly qualified IT resources, and flexibility of IT solutions or access to services powered by mobile technologies.	**EIOPA noted the concerns raised by the respondent.** Within the impact assessment, EIOPA has considered the ICT service industry as direct stakeholder in the development of these Guidelines, however being the ICT industry not directly under EIOPA's remit, EIOPA did not present a direct impact study for the ICT service industry. However, considering that most of the cloud service providers are outsourcers both to the banking and the insurance industry having harmonised these Guidelines with the ones issued by the EBA on outsourcing should minimise the impacts on the IT service industry.
Annex Y/N	
YES	