To the EIOPA Secretariat
EIOPA – Westhafen Tower, Westhafenplatz 1 - 60327 Frankfurt – Germany

On behalf of Google Cloud, we appreciate the opportunity to respond to the EIOPA public consultation on guidelines on outsourcing to cloud service providers. We applaud and share the objective of the guidelines to provide clarity and regulatory certainty to the insurance and reinsurance sector financial institutions on their cloud adoption journey.

The use of cloud-based technologies by small and large organizations is a key pillar of the digital transformation of the economy, driving competitiveness and generating significant economic and social benefits[1]. Cost savings, enhanced collaboration, business agility, AI and advanced data analytics are key benefits that can be realized through cloud adoption. Cloud-based solutions also enhance security as hyperscale cloud providers can offer security capabilities that would be more difficult to manage by, or unavailable to, organisations individually on premise (especially smaller organizations). A recent research from McKinsey & Company[2] concludes that a majority of the 100 enterprise organizations surveyed expect to double their public cloud adoption largely due to the growing understanding that cloud platforms' security capabilities have surpassed those available on the premises. Organizations in the most heavily regulated industries in which data security is a top priority, such as financial services, healthcare, and the public sector already use cloud services and continue migrating more workloads to cloud. The research firm MarketsandMarkets predicts that the finance cloud market will grow at an estimated CACG of 24.4% through 2021.[3]

Whilst financial sector institutions were early adopters of the private cloud, they were relatively slow to migrate to the public cloud due a variety of factors including the complexity of the regulatory landscape and legacy infrastructure. The primary inhibitors commonly cited were security, compliance, and privacy. Nevertheless, adoption of public cloud services has gradually increased over the past few years, as financial institutions have realized the business and security benefits of making the shift, and many initial concerns were eased by the cloud service providers strong compliance programmes. As the global regulatory and compliance landscape evolves, financial organisations have turned to cloud service providers as a means of risk mitigation and for the benefits of an infrastructure that can provide high availability and security capabilities along with data integrity, portability, and confidentiality.

We believe that the draft EIOPA guidelines are reaching an important milestone of harmonizing the approach to outsourcing to cloud in the insurance and reinsurance sector in Europe, consistently with the EBA outsourcing framework. The suggested EIOPA framework takes a balanced risk-based approach accounting for the specific considerations of a multi-tenant global cloud services environment, and recognising the benefits of cloud adoption for the industry.

With this in mind, we have submitted our response to the online questionnaire[4] focusing on the core issues from the perspective of a cloud service provider and based on our contractual commitments to our customers. We would also like to submit the attached detailed response that clarified the rationale of our comments and suggests specific amendments to the draft guideline.
Our response is focused on the following major areas where we believe the draft guidelines could be further improved to facilitate cloud adoption in the insurance and reinsurance sector :

1. Approach to the **data residence policy**: we do not believe it is appropriate to require undertakings to agree a data residency policy with cloud service providers in every case regardless of whether it is an appropriate solution to the identified risks. This will introduce significant barriers to the adoption and use of cloud services by undertakings - in particular those with global operations. This requirement is also inconsistent with the approach to the same issue in the EBA Outsourcing Guidelines where - rather than mandating a data residency policy in all cases - institutions are required to take a risk-based approach to data storage and data processing location(s) and information security considerations. This inconsistency will create regulatory fragmentation that will lead to increased overheads. Finally, there is clear potential for this requirement to overlap and potentially contradict the data transfer requirements in the GDPR.

2. **Access and audit rights**: we believe EIOPA has made significant progress in providing a balanced, risk-based approach to audits and access rights. This will help to address well acknowledged tensions between how audit and access rights need to be framed in the outsourcing agreement and how all parties would expect them to be exercised in practice to preserve the security of the multi-tenant cloud environment. To achieve further certainty in the EIOPA guidelines, we 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. We are suggesting specific amendments in our detailed response attached.

3. **Third-party certifications and audit reports**: third-party certifications and audit reports, such as ISO, SOC etc, provide important information and assurance to customers in a scalable and standardised way. Cloud service providers endeavour to make these resources relevant and helpful to as many customers as possible. If an individual undertaking would like further information, that undertaking can choose to conduct their own individualised assessment with the cloud service provider. It would be infeasible to expect cloud service providers to augment their certifications and audit reports for all customers based on a single undertaking's request. Equally, if different undertakings made different requests, the certifications and reports could lose their relevance to all customers. Making the use of certifications and audit reports conditional on the ability to make such requests could unduly limit the use of these important materials. This would be disproportionate given that, in addition to the certifications and audit reports, the undertakings always has the ability to perform its own assessment.

[1] https://www2.deloitte.com/content/dam/Deloitte/es/Documents/tecnologia/Deloitte_ES_tecnologia_economic-and-social-impacts-of-google-cloud.pdf
[2] McKinsey. Making a Secure Transition to the Public Cloud: https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/McKinsey%20Digital/Our%20Insights/Making%20a%20secure%20transition/Making-a-secure-transition-to-the-public-cloud-full-report.ashx
[3] Finance Cloud Market by Solution (Financial Reporting and Analysis, Security, Governance, Risk and Compliance), Service, Application, Deployment Model, Organization Size, Vertical, Region - Global Forecast to 2021, December 2016
[4] https://ec.europa.eu/eusurvey/runner/Consultation_Cloud_GL_2019

4. **Sub-outsourcers:** we believe the guidelines could benefit from clarifications around sub-outsourcers to account for the practicalities of the cloud environment. Requiring every undertaking to have a right to object to (or veto) a new sub-outsourcer is highly impractical in a multi-tenant environment. We suggest clarifying that the undertaking's "power to object" to sub-outsourcing is exercised using the undertaking's right to terminate. We also suggest changes to the definition of "significant sub-outsourcers" to address the scenario where a cloud service provider engages other providers to provide elements of the cloud service that are not themselves cloud services (e.g. a security provider).

We are submitting suggested amendments to the draft language in the attachment to supplement our response to the online questionnaire, and would be available for a further discussion, should that be of interest.

Kseniia Duxfield-Karyakina

Ksenia Duxfield-Karyakina,

Google Cloud Public Policy and Government Affairs Manager, EMEA
kseniak@google.com

EIOPA CONSULTATION RESPONSE

NB: Column A sets out the EIOPA guideline reference, column B - Google's response and column C - suggested amendments to the guideline text.

EIOPA ref	(A) Draft Guideline	(B) Google response	(C) Google suggestion
Introduction			
Q1. Is the scope of application provided appropriate and sufficiently clear? Q2. Is the set of definitions provided appropriate and sufficiently clear? Q3. Is the timeline to implement the Guidelines considered sufficient to ensure a smooth transition from the current operational practices to the ones provided by these Guidelines?			
1.	In accordance with Article 16 of Regulation (EU) No 1094/2010[5] EIOPA is issuing these Guidelines to provide guidance to insurance and reinsurance undertakings on how the outsourcing provisions set forth in Directive 2009/138/EC[6] ("Solvency II Directive") and in Commission Delegated Regulation (EU) No 2015/35[7] ("Delegated Regulation") needs to be applied in case of outsourcing to cloud service providers. To that end, these Guidelines build 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).		
2.	These Guidelines are addressed to competent authorities and to insurance and reinsurance undertakings (collectively 'undertaking(s)'). The Guidelines apply to both individual undertakings and mutatis mutandis for groups[8]. When the Guidelines refer to entities that are part of the group, in general, they refer to insurance and reinsurance undertakings.		
3.	Undertakings and competent authorities should, when complying or supervising compliance with these Guidelines, take into account the principle of proportionality[9], and the materiality of the service outsourced to cloud service providers. The proportionality principle aims at ensuring that governance		

[5] 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).
[6] 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).
[7] 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).
[8] As defined by Article 212 (1) of Directive 2009/138/EC.
[9] The application of the principle of proportionality, in the context of these Guidelines, should be done in accordance with Article 29 of Directive 2009/138/EC.

	arrangements, including those related to outsourcing to cloud service providers, are consistent with the nature, scale and complexity of their risks.		
4.	These Guidelines should be read in conjunction with and without prejudice to EIOPA Guidelines on system of governance and to the regulatory obligations listed at paragraph 1.		
5.	If not defined in these Guidelines, the terms have the meaning defined in the legal acts referred to in the introduction.		
6.	In addition, for the purposes of these Guidelines, the following definitions apply:		
	Function means any processes, services or activities.		
	Material outsourcing means the outsourcing of critical or important operational functions or activities as further specified by Guideline 7.		
	Outsourcing process means all the activities performed by the undertakings to plan, contract, implement, monitor, manage and terminate outsourcing arrangements.		
	Service provider means a third party entity that is performing an outsourced process, service or activity, or parts thereof, under an outsourcing arrangement.		
	Cloud service provider means a service provider responsible for delivering cloud services under an outsourcing arrangement. 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. The same principle is applied to the cloud brokers.		
	Cloud broker means an entity that manages the use, performance and delivery of cloud services, and negotiates relationships between cloud providers and cloud customers. A cloud customer may request cloud services from a cloud broker, instead of contacting a cloud service provider directly.		
	Significant sub-outsourcer means service provider responsible for delivering cloud services to the main provider with whom the	**Issue**	We suggest amending the guideline as follows:

	undertaking has a contractual agreement in place; a sub-outsourcer is significant when the main agreement would not work without an effective and safe delivery of sub-outsourced services.	Based on the current draft, only a sub-outsourcer who itself provides cloud services (as defined) is considered a "significant sub-outsourcer". **Rationale** The current draft appears to contemplate the scenario where a SaaS provider engages an IaaS provider. Here both providers are providing a "cloud service". Therefore, the IaaS provider is in-scope of the "significant sub-outsourcer" definition. However, a cloud service provider may engage other providers to provide elements of the cloud service that are not themselves cloud services. For example, an IaaS provider may engage a security provider to provide physical security at its IT facilities. Though not cloud services themselves, the security provider provides a key element of the cloud service that, if not delivered effectively, could compromise the cloud service. **Impact** The current draft could lead to confusion about what sub-outsourcers are in scope of the Guidelines. This could lead to inconsistent supervisory practices. This is especially the case given that the EBA Outsourcing Guidelines and the EBA Cloud Recommendations do not limit the rules applicable to sub-outsourcers to those sub-outsourcers who are themselves providing a cloud service.	"Significant sub-outsourcer means a service provider responsible for delivering ~~cloud~~ services (including cloud services) to the ~~main~~ cloud service provider with whom the undertaking has a contractual agreement in place; a sub-outsourcer is significant when the main agreement for cloud services would not work without an effective and safe delivery of sub-outsourced services."
	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.[10]		
	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.		
7.	These Guidelines apply from 01 July 2020 to all cloud outsourcing arrangements entered into or amended on or after this date.		
8.	Undertakings should review and amend accordingly existing cloud outsourcing		

[10] The cloud services are typically delivered to the undertakings in the form of Software as a Service ("SaaS"), Platform as a Service ("PaaS") and Infrastructure as a Service ("IaaS").

	arrangements with a view to ensuring that these are compliant with these Guidelines by 01 July 2022.		
9.	Where the review of material cloud outsourcing arrangements is not finalised by 01 July 2022, an undertaking should inform its supervisory authority[11] of that fact, including the measures planned to complete the review or the possible exit strategy. Then, the supervisory authority may agree with the undertaking on an extended timeline for completing that review where appropriate.		
Guideline 1 – Cloud services and outsourcing			
Q4. Is the Guideline on cloud service and outsourcing appropriate and sufficiently clear to enable the distinction between cloud services falling within the scope of outsourcing and the ones not falling within such scope?			
10.	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:	**Issue** The Guidelines require that authorities and undertakings start from the assumption that all arrangements with cloud service providers are "outsourcing". **Rationale** 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. **Impact** 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.	We suggest amending the Guideline as follows: "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:" In addition, we suggest adding examples of arrangements with cloud service providers that would not be considered "outsourcing". This was the approach taken in the EBA's Outsourcing Guidelines.
a.	whether the function (or a part thereof) outsourced is performed on a recurrent or an ongoing basis; and		
b.	whether this function (or part thereof) would normally fall within the scope of functions that would or could normally be performed by the undertaking in the course of its regular business activities, even if the undertaking has not performed this function in the past.		
11.	Where an arrangement with a service provider covers multiple functions, the undertaking should consider all aspects of the arrangement within its assessment.		

[11] As defined by Article 13 (10) of Directive 2009/138/EC.

12.	As part of their internal control system, taking into account the principle of proportionality and the materiality of the function outsourced, 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.		
Guideline 2 – General Principles of governance for cloud outsourcing			
13.	The decision to enter into a material outsourcing[12] with cloud service providers should be taken by the undertaking's administrative, management or supervisory body (AMSB). That decision should be based on a thorough risk assessment including all relevant risks implied by the arrangement such as IT and operational risks, business continuity risk, legal and compliance risks, concentration risk and, where applicable, risks associated to the data migration and/or the IT implementation phase.		
14.	The undertaking, where appropriate, should reflect the changes on its risk profile due to its cloud outsourcing arrangements within its own risk and solvency assessment ('ORSA').		
15.	The use of cloud services should be consistent with the undertaking's strategies (e.g. IT strategy) and internal policies and processes which should be updated, if needed.		
Guideline 3 – Written policy on outsourcing to cloud service providers			
Q5. Is the Guideline on written policy appropriate and sufficiently clear to manage the undertaking's roles, processes and procedures on outsourcing to cloud service providers? Is it consistent with the market best practices on defining the policy for general outsourcing?			
16.	In case of outsourcing to cloud service providers, the undertaking should update the written outsourcing policy, taking into account cloud computing specificities at least in the following areas:		
a.	the roles and responsibilities of the functions involved in case of outsourcing to cloud service providers (in particular: AMSB, IT function, compliance function, risk management function and internal audit);		
b.	the processes and reporting procedures required for the approval, implementation,		

[12] An undertaking establishes the materiality of its cloud outsourcing arrangements according to the provisions described in Guideline 7.

	monitoring, management and renewal, where applicable, of cloud outsourcing arrangements;		
c.	the oversight of the cloud services including (i) risk assessments and due diligence on cloud service providers, including their frequency; (ii) monitoring and management controls (e.g. verification of the service level agreement); (iii) security standards and controls;		
d.	contractual requirements for material and non-material cloud outsourcing arrangements;	**Issue** As drafted, it is not clear that the reference to "contractual requirements" is a reference to the contractual requirements in Guideline 10. **Rationale** 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: (1) 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 (2) decrease the undertaking's ability to adapt the contractual requirements to the specific arrangement in question. **Impact** 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: (1) Cloud arrangements could be summarily disqualified during due diligence in scenarios where perceived gaps could have been addressed in negotiation. (2) Overall contracts for arrangements with cloud service providers could be less fit-for-purpose.	We suggest amending the Guideline as follows: "(d) contractual requirements in Guideline 10 for material and non-material cloud outsourcing arrangements;"
e.	documentation requirements and written notification to the supervisory authority; and		
f.	documented strategies to exit ('exit strategies') material outsourcing and to terminate ('termination processes') the cloud outsourcing arrangements regardless of their materiality.		
Guideline 4 - Written notification to the supervisory authority			
Q6. Is the list of information to be notified to the national supervisory authorities considered appropriate to understand the most significant areas taken into account by the undertakings in their decision making process?			
17.	The written notification requirement set in Article 49(3) of the Solvency II Directive and further detailed by EIOPA Guidelines on System of Governance (Guideline 64) are		

	applicable to all material cloud outsourcing identified according to Guideline 7.		
18.	The undertaking's written notification to the supervisory authority for material cloud outsourcing should include, in addition to a draft version of the outsourcing agreement, and taking into account the principle of proportionality, at least the following information:		
a.	the function outsourced and its interconnections with other critical or important functions;		
b.	the start date and, as applicable, the next contract renewal date, the end date and/or notice periods for the service provider and for the undertaking;		
c.	the governing law of the cloud outsourcing agreement;		
d.	in case of groups, the insurance or reinsurance undertakings and other undertakings within the scope of the prudential consolidation, where applicable, that make use of the cloud services;		
e.	the name of the 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;		
f.	a description of the activities performed by the cloud service provider, the cloud service models (for example IaaS/PaaS/SaaS), the cloud infrastructure (i.e. public/private/hybrid/community), the specific nature of the data to be held and the locations (i.e. countries or regions) where such data will be stored and processed, the results of the materiality assessment and the date of the more recent materiality assessment;	**Issue** The reference to locations where data are "processed" will be problematic if the word "processed" in the Guidelines is given the same meaning as it is under the GDPR. **Rationale** "Process" is defined widely in the GDPR. It would include data transport / transit. Specifying the countries / 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. **Impact** 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.	We suggest amending the Guideline as follows: "a description of the activities performed by the cloud service provider, the cloud service models (for example IaaS/PaaS/SaaS), the cloud infrastructure (i.e. public/private/hybrid/community), the specific nature of the data to be held and the locations (i.e. countries or regions) where such data will be stored and processed (except locations through which data merely transit), the results of the materiality assessment and the date of the more recent materiality assessment;"

g.	the outcome of the assessment of the cloud service provider's substitutability (e.g. easy, difficult or impossible);		
h.	whether the undertaking has an exit strategy in case of termination by either party or disruption of services by the cloud service provider, in line with EIOPA Guidelines on System of Governance (Guideline 63);		
Guideline 5 – Documentation requirements			
Q7. 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? What can be other approaches to ensure a proper and sound holistic oversight of cloud outsourcing? Q8. Are the documentation requirements appropriate and sufficiently clear?			
19.	As part of their governance and risk management systems, the undertaking should maintain an updated register on all its material and non-material functions outsourced to cloud service providers. Taking into account national regulation and the principle of proportionality, the undertaking should maintain the documentation of past outsourcing arrangements within the register and the supporting documentation for an appropriate retention period.		
20.	The undertaking should make available to the supervisory authority, on request, the register, a copy of the outsourcing agreement, and related information on the periodical assessment performed, or any parts thereof.		
21.	Where the register of all existing cloud outsourcing arrangements is established and maintained centrally within a group, supervisory authorities and all undertakings belonging to the group should be able to obtain the section of the register related to an individual undertaking without undue delay.		
22.	In case of non-material outsourcing, the register should include, where applicable, the information to be notified to the supervisory authority for material cloud outsourcing arrangements referred to in Guideline 4.		
23.	In case of material outsourcing, the register should include at least the following information:		
a.	the information to be notified to the supervisory authority for material cloud outsourcing arrangements referred to at Guideline 4;		

b.	the date of the latest risk assessment and a brief summary of the main results;		
c.	the decision-making body (e.g. the management body) in the undertaking that approved the cloud outsourcing;		
d.	the estimated annual costs;		
e.	the dates of the most recent and next scheduled audits, where applicable;		
f.	the names of significant sub-outsourcers, if any, including the countries where the sub-outsourcers are registered, where the service will be performed and, if applicable, the locations (i.e. countries or regions) where the data will be stored and processed;	Please see our comments on paragraph 18(f) about the reference to “processed”.	We suggest amending the Guideline as follows: “the names of significant sub-outsourcers, if any, including the countries where the sub-outsourcers are registered, where the service will be performed and, if applicable, the locations (i.e. countries or regions) where the data will be stored and processed (except locations through which data merely transit);”
g.	whether the cloud service provider (or any significant sub-outsourcer(s)) supports business operations that are time critical;		
h.	whether the cloud service provider (or any significant sub-outsourcer(s)) has a business continuity plan that is suitable for the services provided to the undertaking in line with Article 274(5)(d) of the Delegated Regulation; and	**Issue** Please see our comments on paragraph 6 on the definition of “significant sub-outsourcer”. If, as we suggest, the definition of “significant sub-outsourcer” is adjusted to include sub-outsourcers who are not providing a cloud service, then as drafted this Guideline would require the undertaking to include information about a non-cloud service sub-outsourcer’s business continuity plan in the register. **Rationale** If a significant sub-outsourcer provides a cloud service to the main cloud service provider, then in practice the significant sub-outsourcer’s own business continuity plan is likely to be relevant to the availability of the data hosted on the main cloud service. However, if a significant sub-outsourcer does not provide a cloud service, then it is unclear how their business continuity plan is directly relevant to the availability of the data hosted on the main cloud service in practice. The main cloud service provider’s own business continuity plan will address the loss / interruption of the non-cloud sub-sourced service (e.g. a loss of third party provider is typically one of the business continuity scenarios that the cloud service provider’s business continuity plan is designed to address). **Impact** Requiring undertakings to assess the business continuity plans of significant sub-outsourcers who are not providing a cloud service would be disproportionate as in practice the loss / interruption of non-cloud sub-outsourced services should be addressed in the cloud service provider’s own business continuity plan.	We suggest amending the Guideline as follows: “whether the cloud service provider or (if applicable any significant sub-outsourcer(s) responsible for delivering a cloud service to the main provider) has a business continuity plan that is suitable for the services provided to the undertaking in line with Article 274(5)(d) of the Delegated Regulation; and”
i.	a description of the undertaking monitoring of the cloud outsourced activities (i.e. number of resources and their skills).		

Guideline 6 – Pre-outsourcing analysis			
24.	Before entering into any arrangement with cloud service providers, the undertaking should:		
a.	assess if the cloud outsourcing arrangement is material;		
b.	identify and assess all relevant risks of the cloud outsourcing arrangement;	**Issue** As drafted, it is not clear that the reference to identifying and assessing "all relevant risks" is a reference to the risk assessment in Guideline 8. **Rationale** This 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. **Impact** This could lead to divergent practices by undertakings and authorities because of the potential for different interpretations.	We suggest amending the Guideline as follows: "perform the risk assessment required by Guideline 8 ~~identify and assess all relevant risks of the cloud outsourcing arrangement;~~"
c.	undertake appropriate due diligence on the prospective cloud service provider; and		
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 – Materiality assessment			
Q9. Taking into account the specific nature of cloud services, it has been opted to use the concept of 'materiality' to clarify, in this context, the one of 'critical or important operational function'. Is this approach appropriate and sufficiently clear?			
25.	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.		
26.	The undertaking should consider always as material all the outsourcing of critical or important operational functions to cloud service providers. The identification of critical or important operational functions should be		

	performed according to EIOPA Guidelines on System of Governance (Guideline 60)[13]		
27.	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:		
a.	the potential impact of outages, disruptive events or failure of the cloud service provider to provide the services at the agreed service levels on the undertaking:		
(i)	continuous compliance with the conditions of their authorization, and other obligations under the Solvency II Directive;		
(ii)	short and long-term financial and solvency resilience and viability;		
(iii)	business continuity and operational resilience;		
(iv)	operational risk, including conduct, information and communication technology (ICT), cyber and legal risks;		
(v)	reputational and strategic risks;		
(vi)	recovery and resolution planning, resolvability and operational continuity in an early intervention, recovery or resolution situation, where applicable.		
b.	the potential impact of the cloud outsourcing arrangement on the ability of the undertaking to:		
(i)	identify, monitor and manage all risks;		
(ii)	comply with all legal and regulatory requirements;		
(iii)	conduct appropriate audits regarding the function affected by the cloud outsourcing arrangement, in line with Article 38 of the Solvency II Directive;		
c.	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;		

[13] "The undertaking should determine and document whether the outsourced function or activity is a critical or important function or activity on the basis of whether this function or activity is essential to the operation of the undertaking as it would be unable to deliver its services to policyholders without the function or activity."

d.	the size and complexity of any undertaking's business areas affected by the cloud outsourcing arrangement;		
e.	the cost of the cloud outsourcing as a proportion of total operating and ICT costs of the undertaking;		
f.	the potential business interconnections between the undertakings and the cloud service provider. For instance, if the undertaking is providing (re)insurance coverage to the cloud provider;		
g.	the ability, if necessary or desirable, to transfer the proposed cloud outsourcing arrangement to another cloud service provider or reintegrate the services ('substitutability'); and		
h.	the protection of personal and non-personal data and the potential impact of a confidentiality breach or failure to ensure data availability and integrity on the undertaking, policyholders or other relevant subjects including but not limited to compliance with Regulation (EU) 2016/679[14]. The undertaking should particularly take into consideration data that is business sensitive and/or critical (e.g. policyholders' health data).		
Guideline 8 – Risk assessment of cloud outsourcing			
Q10. Is the content of Guideline on risk assessment of cloud outsourcing appropriate and sufficiently clear?			
28.	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.		
29.	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. The cost-benefit analysis should consider and weigh any significant risks which may be reduced or better managed against any		

[14] 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).

	significant risks which may arise as a result of the proposed cloud outsourcing arrangement.		
30.	Carrying out the risk assessment, the undertaking should, at a minimum:		
a.	consider the design of the cloud service used;		
b.	identify and classify the relevant functions and related data and systems as to their sensitivity and required security measures;		
c.	assess the risks arising from the selected cloud service (i.e. IaaS/PaaS/SaaS) and deployment models (i.e. public/private/hybrid/community);		
d.	where applicable, assess the risks arising from the migration and/or the implementation;		
e.	conduct a thorough risk-based analysis of the functions and related data and systems which are under consideration to be outsourced or have been outsourced and address the potential risk impacts, in particular the operational risks, including legal, IT, compliance and reputational risks, and the oversight limitations related to the countries where the outsourced services are or may be provided and where the data are or are likely to be stored or processed;		
f.	consider the consequences of where the cloud service provider is located, the data are stored or processed (within or outside the EU) including the context of assuring compliance of the provided services with applicable EU and national laws, external and internal regulations and standards adopted by the undertaking;	Please see our comments on paragraph 18(f) about the reference to “processed”.	We suggest amending the Guideline as follows: “consider the consequences of where the cloud service provider is located, the data are stored or processed (except locations through which data merely transit) (within or outside the EU) including the context of assuring compliance of the provided services with applicable EU and national laws, external and internal regulations and standards adopted by the undertaking;”
g.	consider the political stability and security situation of the jurisdictions in question, including:		
(i)	the laws in force, including laws on data protection;	**Issue** This Guideline should also refer to whether the conditions for transfer of personal data to a third country under the GDPR are met. **Rationale** If personal data are involved, considering whether the conditions for transfer of personal data to a third country under the GDPR are met (and in particular if a recognised compliance mechanism applies to the transfer) is	We suggest amending the Guideline as follows: “the laws in force, including laws on data protection and where personal data are involved, whether the conditions for transfer of personal data to a third country under the GDPR are met;”

		essential to assessing the potential legal risks and compliance issues. As such it will be a critical part of any risk-based approach to consideration of data processing locations in the context of cloud outsourcing. **Impact** As drafted, this Guideline does not take the opportunity to achieve further convergence on how undertakings should assess data processing locations in the context of cloud outsourcing and to align this assessment with the GDPR. This may lead to incomplete risk assessments due to a lack of consideration of valid transfer mechanisms under the GDPR. This could in turn lead to fragmentation as undertakings consider their obligations for data transfers under both regimes.	
(ii)	the law enforcement provisions in place; and		
(iii)	the insolvency law provisions that would apply in the event of a service provider's failure and any constrains that would arise in the respect of the urgent recovery of the undertaking's data in particular;		
h.	assess the risk of significant sub-outsourcing by the cloud service provider, taking into account:		
(i)	the risks associated with sub-outsourcing, including the additional risks that may arise if the sub-outsourcer is located in a third country or a different country from the service provider;		
(ii)	the risk that long and complex chains of sub-outsourcing reduce the ability of the undertaking to oversee its material function and the ability of supervisory authorities to effectively supervise them;		
	The risk management system applied by the undertaking should take into account the risks related to sub-outsourcing. If the risk is considered too high, the undertaking should not accept sub-outsourcing to a specific sub-outsourcer or third party.		
i.	assess the concentration risk, including from:		
(i)	outsourcing to a dominant cloud service provider that is not easily substitutable; and		
(ii)	multiple outsourcing arrangements with the same cloud service provider or closely connected service providers;		
31.	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). Moreover, if the undertaking becomes aware of significant		

	deficiencies and significant changes of the services provided or the situation of the cloud service provider, the risk assessment should be promptly reviewed or re-performed.		
Guideline 9 – Due diligence on cloud service provider			
32.	Undertakings should perform a due diligence on the cloud service provider applying criteria defined by their written outsourcing policy.		
33.	The due diligence should include an evaluation of the suitability of the cloud provider (skills, infrastructure, economic situation, corporate and regulatory status, etc.). Where appropriate, evidence / certificates based on common standards (including but not necessarily limited to: International Safety Standard ISO / IEC 2700X of the International Organization for Standardization, C 5 Requirement Catalogue of the Federal Office for Information Security), test reports of recognized third parties or internal test reports of the cloud provider can be used to support the due diligence performed.		
Guideline 10 – Contractual requirements			
Q11. Are the contractual requirements for material outsourcing appropriate and sufficiently clear? Q12. Are the criteria provided to set the contractual requirements for non-material outsourcing appropriate and sufficiently clear?			
34.	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.		
35.	In addition to the set of requirements defined by Article 274 of the Delegated Regulation, the written agreement between an undertaking and a cloud service provider for arrangements classified as material should set out at least:		
a.	a clear description of the cloud services, including the type of support services;		
b.	the start date and, as applicable, the next contract renewal date, the end date and/or notice periods for the service provider and for the undertaking;		
c.	the court jurisdiction and the governing law of the agreement;		
d.	the parties' financial obligations including the cloud services pricing model;		

e.	the parties' operational obligations and responsibilities (for example, in case of updates or in case of user and access management or incident management);		
f.	whether significant sub-outsourcing is permitted, and, if so, the conditions to which the sub-outsourcing is subject to (see Guideline 13);		
g.	the location(s) (i.e. regions or countries) where relevant data will be kept and processed, including the possible storing locations (i.e. location of data centres), and the conditions to be met, including a requirement to notify the undertaking if service provider proposes to change the location(s)	**Issue** It is not clear what is meant by "kept" and how this is different to "storing". **Rationale** 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". **Impact** This could create uncertainty for both undertakings and cloud service providers. Without clarification, this Guideline could also lead to authorities taking different interpretations. In addition, please see our comments on paragraph 18(f) about the reference to "processed".	We suggest amending the Guideline as follows: "the location(s) (i.e. regions or countries) where relevant data will be stored ~~kept~~ and processed~~, including the possible storing locations~~ (except locations through which data merely transit)(i.e. location of data centres), and the conditions to be met, including a requirement to notify the undertaking if service provider proposes to change the location(s)"
h.	provisions regarding the accessibility, availability, integrity, confidentiality, privacy and safety of relevant data, taking into account the specifications of Guideline 12;		
i.	the right for the undertaking to monitor the cloud service provider's performance on an on-going basis taking into account the Guideline 14;		
j.	the agreed service levels which should include quantitative and qualitative performance targets, that are directly measurable by the undertaking in order to independently monitor the services received and, eventually, adopt corrective action if agreed service levels are not met;		
k.	the reporting obligations of the cloud service provider to the undertaking, including the obligations to submit the reports relevant for the undertaking's internal audit function;		
l.	whether the cloud service provider should take mandatory insurance against certain risks and, if applicable, the level of insurance cover requested;		

m.	the requirements to implement and test business contingency plans;		
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.		
36.	Regarding an outsourcing agreement for material cloud outsourcing, special care should be taken of Article 274(4)(h) to (l) 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.	**Issue** It is not clear what extra steps an undertaking would need to take in order to take 'special care'. **Rationale** 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. **Impact** This could create uncertainty for both undertakings and cloud service providers. Without clarification, this Guideline could also lead to authorities taking different interpretations.	We suggest amending the Guideline as follows: “Regarding an outsourcing agreement for material cloud outsourcing, ~~special care~~ undertakings should ensure that the requirements ~~be taken~~ of Article 274(4)(h) to (l) 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 are observed.”
37.	Moreover, regardless the materiality of the outsourcing, the outsourcing agreement should include all the requirements set out in Article 38 of the Solvency II Directive. In particular, the undertaking should ensure that the outsourcing agreement or any other contractual arrangement do not impede or limit its supervisory authority to carry out its supervisory function and objectives and the effective supervision of outsourced functions and activities.		
38.	In case of non-material outsourcing, the clauses within the agreement between the undertaking and a cloud service providers 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).		
Guideline 11 – Access and audit rights			
Q13. Are the guidelines on access and audit rights appropriate and sufficiently clear?			
39.	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	**Issue** This first sentence of this paragraph is unclear. Without clarification any procedural step (e.g. identity verification, security checks) could be interpreted as a limitation on the access and audit rights regardless of the fact that it has no impact on the effective exercise of those rights and in many cases enhances the effective exercise of those rights.	We suggest that this Guideline refer to limits on the effective exercise of the undertaking’s access and audit rights as follows: “The outsourcing agreement should not limit the undertaking’s effective exercise of information, access and audit rights as well as control options on cloud services in order to fulfil all its regulatory obligations.

	risks associated with cloud outsourcing arrangements.	**Rationale** Procedural steps such as identity verification and security checks do not limit an undertakings access and audit rights. To the contrary, they are necessary practical steps to ensure undertakings can exercise their access and audit rights effectively and in a way that limits the risk to the undertaking's cloud environment and the cloud service provider's other customers' environments. **Impact** Without clarification this Guideline could create tension between the description of the audit and access rights in the outsourcing agreement and how all parties would expect audit and access to take place in practice. Not only will this create friction in negotiation that will slow down the adoption of cloud. It could also create real risks to the undertaking's cloud environment in practice.	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." This is the approach taken in the EBA Outsourcing Guidelines. It also reflects the text of Article 38 of the Solvency II Directive and Article 274 of the Delegated Regulation.
40.	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.		
41.	The scope of the audits 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.		
42.	In determining the frequency of audit assessment, the undertaking should consider the nature and extent of risk and impact on the undertaking from the cloud outsourcing arrangements.		
43.	If the performance of audits or the use of certain audit techniques might create a risk for the environment of the cloud service provider and/or another cloud service provider's client (e.g. 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 to the undertaking.		
44.	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 organizational 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), audit performed by third clients or by a third party appointed by them.		
45.	Undertakings should make use of the method referred to in paragraph 44(a) only if they:		
a.	are satisfied with the audit plan for the service outsourced to cloud service providers;		
b.	ensure that the scope of the certification or the audit report covers the systems (i.e. processes, applications, infrastructure, data centres, etc.) and the key controls identified by the undertaking and the compliance with relevant regulatory requirements;		
c.	thoroughly assess the content of new certifications or audit reports on an ongoing basis and verify that the reports or certifications are not obsolete;		
d.	ensure that key systems and controls are covered in future versions of the certification or audit report;		
e.	are satisfied with the aptitude of the certifying or auditing party (e.g. with regard to rotation of the certifying or auditing company, qualifications, expertise, re-performance/verification of the evidence in the underlying audit file);		
f.	are satisfied that certifications are issued and the audits are performed according to appropriate standards and include a test of the operational effectiveness of the key controls in place;		
g.	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; and	**Issue** It should not be a condition of making use of third-party certifications and audit reports that the undertaking has the contractual right to request the expansion of their scope. **Rationale** In a public cloud context, third-party certifications / reports are a way of providing important information to customers in a scalable way. By performing these assessments against accepted international standards, cloud service providers ensure they meet the needs of as many customers as possible. This in turn helps to manage the operational burden and risk associated with individual assessments that are required to produce these materials. It would be disproportionate to expect the cloud service provider to expand the scope of the certifications/reports for a single undertaking. If each undertaking makes different requests, this could result in bespoke certifications / reports for each undertaking. This would necessarily require individualised	We suggest deleting this subsection.

		assessments. As a result, the certifications / reports would lose their relevance to all customers and their effectiveness as a scalable compliance tool. If the undertaking believes there is a gap in existing internationally-accepted standards on which the certifications/reports are based or if their own internal risk framework goes beyond internationally-accepted standards, undertakings can exercise their access and audit rights to address that gap per Guideline 45(h). In addition, as a long term solution, undertakings should advocate to the standards body that manages the relevant standard to change it to address any material gaps. **Impact** Making this a condition for undertakings using third party certifications and reports may unduly limit the use of certifications and reports. Alternatively, if cloud service providers agree to offer this right, there is a real risk that (1) certifications and audit reports will lose their relevance to all customers and will become individualised and bespoke, and (2) providers will have to perform multiple assessments to satisfy each institution's expanded requirements.	
h.	retain the contractual right to perform individual on-site audits at their discretion with regard to material outsourcing; such right should be exercised in case of specific needs not manageable through other types of interactions with the cloud service provider.		
46.	For material cloud outsourcing, the undertaking should assess whether third-party certifications and reports as referred to in paragraph 44(a) are adequate and sufficient to comply with their regulatory obligations but should not rely solely on these reports over time.		
47.	Before a planned on-site visit, the party to exercise its right of access (undertaking, auditor or third party acting on behalf of undertaking(s)) should provide prior notice in a reasonable time period of the on-site visit to a relevant business premise, unless an early prior notification has not been possible due to an emergency or crisis situation.	**Issue** It is not clear what information the prior notice should contain. **Rationale** To ensure the effectiveness of the audit and manage the risk to the cloud environment, prior notice should provide at least the following information about the on-site visit: (1) the location(s) of interest; (2) the time of the visit; (3) the purpose of the visit (i.e. what controls are in scope); and (4) the personnel that will participate in the visit. This information is required for planning, which in turn enhances the effectiveness of the audit. For example, with this information, the cloud service provider can ensure: (1) the audit participants have access to premises in a secure way, (2) the relevant provider personnel are available, and (3) take any other preparatory steps to facilitate the audit. **Impact** Without clarification, a cloud service provider's request for information about the purpose of the visit and personnel that will participate could be mistakenly interpreted as a limit on the access right. This will create	We suggest amending the Guideline as follows: "Before a planned on-site visit, the party to exercise its right of access (undertaking, auditor or third party acting on behalf of undertaking(s)) should provide prior notice in a reasonable time period of the on-site visit to a relevant business premise, 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."

		friction in negotiation that will slow down the adoption of cloud. It could also reduce the effectiveness and efficiency of audits in practice.	
48.	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 effective and relevant audits and/or assessments.		
Guideline 12 – Security of data and systems			
Q14. Are the provisions set by this Guideline for security of data and systems appropriate and sufficiently clear?			
49.	The undertaking should ensure that cloud service providers comply with appropriate IT security and data protection standards. The undertaking should, additionally, define data and system security requirements in the outsourcing agreement and monitor compliance with these requirements on an ongoing basis.		
50.	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:		
a.	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;		
b.	ensure specific measures where necessary for data in transit, data in memory and data at rest, such as the use of encryption technologies in combination with an appropriate key management, and a sound user and access management process;		
c.	ensure that network traffic availability and expected capacity are guaranteed, where applicable and feasible;		
d.	define and decide on proper continuity requirements ensuring adequate levels at each level of the technological chain including significant sub-outsourcing, where applicable;		

e.	define specific processes by the undertaking and the cloud service provider to ensure an overall sound management of the incidents that may occur;		
f.	agree on a data residency policy with the cloud service provider which sets out the countries where the undertaking's data can be stored, processed and managed. This policy should be reviewed periodically and the undertaking should be able to verify compliance of the cloud service provider with such policy; and	**Issue** 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" **Rationale** <u>Addressing risk</u> 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. <u>Effective access</u> 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. 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). **Impact** <u>Practical challenges</u> 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.	We suggest amending the Guideline as follows: "for material cloud outsourcing and where applicable and feasible based on a risk-based approach, agree on a data residency policy with the cloud service provider which sets out the countries where the cloud service provider can elect to store, process (excluding countries through which data merely transit) and manage the undertaking's data ~~can be stored, processed and managed~~. This policy should be reviewed periodically and the undertaking should be able to verify compliance of the cloud service provider with such policy; and"

		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 exands. 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. <u>Harmonisation</u> 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.	
g.	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.		
Guideline 13 – Sub-outsourcing			
51.	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.		
52.	The undertaking should agree to sub-outsource only if the sub-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.		
53.	The cloud outsourcing agreement between the undertaking and the cloud service provider should specify any types of activities that are excluded from potential suboutsourcing and indicate that the cloud service provider retains full responsibility and oversight obligations for the services it has sub-outsourced.		

54.	The cloud outsourcing agreement should also include an obligation for the cloud service provider to inform the undertaking of any planned significant changes to the sub-outsourcers or the sub-outsourced services that might affect the ability of the service provider to meet its responsibilities under the cloud outsourcing agreement. The notification period for those changes should be contractually pre-agreed to allow for 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 suboutsourced services comes into effect.		
55.	In case a cloud service provider plans changes to a sub-outsourcer or suboutsourced services that would have an adverse effect on the risk assessment of the agreed services, the undertaking should have the power to object to such changes and the right to terminate the contract.	**Issue** It is not clear whether the “power to object” is different / additional to the undertaking’s right to terminate the contract. **Rationale** As the EBA acknowledges in the Cloud Recommendations, a right for a single undertaking to veto a sub-outsourcer would be overly burdensome from a practical perspective in the context of outsourcing to public cloud service providers. For context, when a public cloud service provider sub-outsources an element of the service, this sub-outsourcing could potentially apply to all the cloud service provider’s customers. If each customer had a right to veto the new sub-outsourcer, the cloud service provider would only be able to proceed if every single customer consented / did not object. The absence of a veto right does not expose the undertaking to undue risk given: (1) the provider is required to notify the undertaking in advance of planned changes, and (2) the undertaking will have the right to terminate under this Guideline. **Impact** There will be uncertainty about whether a veto right is required. Without clarification, this Guideline could also lead to authorities taking different interpretations. This will be a significant barrier to undertakings using cloud services.	We suggest amending the Guideline as follows: “In case a cloud service provider plans changes to a sub-outsourcer or suboutsourced services that would have an adverse effect on the risk assessment of the agreed services, the undertaking should have ~~the power to object to such changes and~~ the right to terminate the contract.”
Guideline 14 – Monitoring and oversight of cloud outsourcing arrangements			
56.	The undertaking should monitor the performance of activities, the security measures and the adherence to the agreements of their cloud providers on an ongoing basis. In order to do so, the undertaking should set up monitoring and oversight mechanisms. These include but are not limited to the management of:		
a.	the incidents occurred to the cloud provider with impact on the undertaking’s activities;		

b.	data and information governance systems around the processes performed on the cloud;		
c.	the business continuity of the technological and supply chain;		
d.	the mechanisms ensuring integration of the cloud services with the systems of the undertakings; for example, the APIs (Application Programming Interface) and the user and access management process;		
e.	roles and responsibilities between the cloud service provider and the undertaking in relation to all the IT (including IT security and cybersecurity) and non-IT processes affected by the cloud outsourcing, which should be clearly splitted;		
f.	on-going and independent verifications of the Service Level Agreements, which should be agreed with the cloud service provider.		
57.	The undertaking should perform the activities detailed in the previous paragraph taking into account the principle of proportionality and the presence of significant sub-outsourcing, if any.		
58.	The AMSB should be regularly updated on the risks identified in respect of the material outsourcing. As part of this activity, undertakings should monitor and manage their concentration risk caused by cloud outsourcing arrangements.		
59.	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 IT and business knowledge as deemed necessary.		
Guideline 15 – Termination rights and exit strategies			
60.	In addition to the requirements set out in the Delegated Regulation, within the cloud outsourcing agreement, at least for material outsourcing, 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, an undertaking should:		
a.	develop exit plans that are comprehensive, service based, documented and sufficiently tested where appropriate;		
b.	identify alternative solutions, where appropriate and feasible, and develop 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 and taking the necessary measures to ensure business continuity during the transition phase;		
c.	ensure that the cloud service provider and its significant sub-outsourcers (if applicable) adequately supports the undertaking when transferring the outsourced data, systems or applications to another service provider or directly to the undertaking; and;		
d.	agree with the cloud service provider that once retransferred to the undertaking, its data will be completely and irrevocably deleted by the cloud service provider.	**Issue** From a strict technical perspective, the reference to irrevocable deletion is problematic, and may not be fully consistent with the practical intention of the Guidelines. **Rationale** There is not an established understanding from a technological perspective regarding when data can be said to be irrevocably deleted. In particular, some technologists take the view that data can only be said to be irrevocably deleted when the relevant hardware is decommissioned and destroyed. In the public cloud context the hardware is multi-tenant and is only decommissioned at end of life / refresh and not when a single customer marks their data for deletion. When a customer requests for their data to be deleted from Google Cloud, we initiate a documented, secure technological process that is detailed in our Deletion whitepaper[15]. Data marked for deletion is logically deleted from active systems and expired from backup systems via overwriting and cryptographic techniques. This is a standard process recognised and followed across the industry, which we believe meets the intended requirements of the EIOPA Guidelines and our customers at large. The suggested language in the current draft of the Guidelines may be going beyond their practical intention as we do not believe, for example, that it is EIOPA's intention to require hardware to be decommissioned when an undertaking terminates an arrangement with a cloud service provider. This would be disproportionate. It is also unlikely to align with the undertaking's own approach to deletion for data stored in-house. **Impact** The reference to irrevocable deletion could lead to undertakings, cloud service providers and authorities taking different interpretations. Any of these parties could - in good faith - understand the reference to require that	We suggest amending the Guideline as follows: (d) agree with the cloud service provider that once retransferred to the undertaking, its data will be completely and ~~irrevocably~~ securely deleted by the cloud service provider.

[15] https://cloud.google.com/security/deletion/

		hardware is decommissioned and destroyed. Not only will this create friction in negotiation, it could be a significant barrier to undertakings using cloud services.	
61.	When developing exit strategies, the undertaking should consider the following:		
a.	define objectives of the exit strategy;		
b.	define the trigger events (e.g. 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 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; and		
e.	define success criteria of the transition.		
Guideline 16 – Supervision of cloud outsourcing arrangements by supervisory authorities			
62.	The analysis of the impacts arising from undertakings' cloud outsourcing arrangements should be performed by the supervisory authorities as part of their supervisory review process.		
63.	Supervisory authorities should include the supervision of undertakings' cloud outsourcing arrangements in the context of the following risks:		
a.	operational risk (including legal and compliance risk, outsourcing and third party management risk);		
b.	IT risks;		
c.	reputational risk; and		
d.	strategic risk.		
64.	Within their assessments, supervisory authorities should assess 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 with particular focus on material outsourcing;		
b.	whether the undertaking has sufficient resources with adequate skills and knowledge to monitor the services outsourced to the cloud, with particular focus on material outsourcing; and		
c.	whether the undertaking identifies and manages all the relevant risks highlighted by these Guidelines including the concentration risk within the undertaking or the group and at country/sectoral level.		
65.	In case of groups, the group supervisor should ensure that the impacts of material cloud outsourcing[16] are reflected into the group supervisory risk assessment taking into account the requirements listed at the previous two paragraphs and the group specific governance and operational characteristics. In light of the above, in the context of material cloud outsourcing that involves more than one undertaking in different Member states 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 IT provider), the group supervisor and/or the relevant supervisory authorities of the undertakings involved in the proposed cloud outsourcing, should discuss, where appropriate, the impacts to the group risk profile of the cloud outsourcing in the context of the College of Supervisors[17]		
66.	In case of on-site inspections carried out at cloud service providers' premises by the supervisory authorities, without prejudice to the requirements set out in the Solvency II Directive, Guideline 31 of the EIOPA Guidelines on supervisory review process (EIOPA-BoS-14/179) and other regulatory requirements that may apply, the supervisory authorities should have the adequate mix of knowledge and experience to perform supervision of this type of requirements (such as, for example, IT and technology knowledge, IT security & cybersecurity, business continuity management, governance and third party risk management, knowledge of legal and compliance requirements of the jurisdictions where the assessment is performed).		

[16] The materiality of cloud outsourcing is established according to the provisions described in Guideline 7.
[17] As defined in Article 212(1) sub (e) of Directive 2009/138/EC.

67.	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: improving the governance arrangement, limiting or restricting the scope of the outsourced functions or requiring 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 the supervision and enforcement of regulatory requirements cannot be ensured by other measures.		
Compliance and reporting rules			
68.	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.		
69.	Competent authorities that comply or intend to comply with these Guidelines should incorporate them into their regulatory or supervisory framework in an appropriate manner.		
70.	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.		
71.	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			
Q15. Are the requirements set by these Guidelines and in particular by Guidelines 4 and 5 on notification and documentation requirements sufficiently proportionate? EIOPA welcomes concrete operational examples as to how to ensure that the principle of proportionality is effectively reflected in these Guidelines.			
72.	The present Guidelines will be subject to a review by EIOPA.		