Consultation paper Non the proposal19/270 for Guidelines on outsourcing to cloud service providers

Guidelines on outsourcing to cloud service providers

Introduction

1. In accordance with Article 16 of Regulation (EU) No ~~1094/2010[4]~~1094/20106 EIOPA ~~is issuing these~~issues Guidelines to provide guidance to insurance and reinsurance undertakings on how the outsourcing provisions set forth in Directive ~~2009/138/EC[5]~~2009/138/EC7 ("Solvency II Directive") and in Commission Delegated Regulation (EU) No ~~2015/35[6]~~2015/358 ("Delegated Regulation") needs to be applied in case of outsourcing to cloud service providers. ~~To that end,~~2. these Guidelines ~~build~~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).

~~2.~~3. These Guidelines are addressed to competent authorities ~~and to~~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 for ~~groups[7]. When the Guidelines refer to entities that are part of the group, in general, they refer to insurance and reinsurance undertakings.~~groups. 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. ~~3.~~ Undertakings and competent authorities should, when complying or supervising compliance with these Guidelines, take into account the principle of ~~proportionality[8], and the materiality~~ proportionality10 and the criticality or importance of the service outsourced to cloud service providers. The proportionality principle ~~aims at ensuring~~should ensure that governance arrangements, including those related to outsourcing to cloud service providers, are ~~consistent with~~proportionate to the nature, scale and complexity of ~~their~~the underlying risks.

~~4.~~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 ~~at paragraph 1.~~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.~~5.~~ If not defined in these Guidelines, the terms have the meaning defined in the legal acts referred to in the introduction.

~~6.~~9. 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~~a 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.~~, as defined above, responsible for delivering cloud services under an outsourcing arrangement
~~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 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~~.
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[9].~~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.

~~7.~~Date of application 10. These Guidelines apply from ~~01 July 2020~~1 January 2021 to all cloud outsourcing arrangements entered into or amended on or after this date.

~~8.~~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 ~~that these are compliant~~compliance with these Guidelines by ~~01 July~~31 December 2022.

~~9~~12.. Where the review of ~~material~~ cloud outsourcing arrangementsrelated to critical or important operational functions or activities is not finalised by ~~01 Jul~~31 Decembery 2022, ~~a~~then undertaking should inform its supervisory ~~authority[1]~~authority11[0] of that fact, including the measures planned to complete the review or the possible exit strategy. ~~Then, th~~The supervisory authority may agree with the undertaking on an extended timeline for completing that review where appropriate.

~~Questions to stakeholders~~

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.

~~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?~~

Guideline 1 – Cloud services and outsourcing

~~10.~~14. The undertaking should establish whether an arrangement with a cloud service provider falls under the definition of outsourcing ~~(Article 13(28) of~~pursuant to the Solvency II Directive~~). As a rule, outsourcing should be assumed~~. 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 part thereof) would normally fall within the scope of operational functions or activities 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 operational function or activity in the past.

~~11.~~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.

~~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.~~

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

~~Questions to stakeholders~~

~~Q4. Is the Guideline on cloud services and outsourcing appropriate and sufficiently clear to enable the distinction between~~ cloud services ~~falling within the scope~~provider is part of a sub-outsourcing ~~and~~chain), the ~~ones not falling~~arrangement for such outsourcing falls within ~~such~~the scope~~?~~ of these Guidelines.

Guideline 2 - General principles of governance for cloud outsourcing

~~13. The decision to enter into a material outsourcing[11] with cloud service providers should be taken by~~

17. Without prejudice to Article 274(3) of the Delegated Regulation, the undertaking's administrative, management or supervisory body (AMSB). ~~That decision should be~~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 ~~IT and operational risks~~information and communication technology ("ICT"), business continuity ~~risk~~, legal and compliance ~~risks~~, concentration ~~risk and, where applicable,~~, other operational risks, and risks associated to the data migration and/or the ~~IT~~ implementation phase, ~~14. Th~~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 on its risk profile due to its cloud outsourcing arrangements ~~withi~~in its own risk and solvency assessment ('ORSA').

~~15.~~19. The use of cloud services should be consistent with the undertaking's strategies (~~e.g. IT~~for example, ICT strategy, information security strategy, operational risk management strategy) and internal policies and processes which should be updated, if needed.

Guideline 3 – ~~Written policy on~~Update of the outsourcing ~~to cloud service providers~~written policy

20.~~16.~~ 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 ~~computing~~outsourcing specificities at least in the following areas:

c. the roles and responsibilities of the undertaking's functions involved in ~~case of outsourcing to cloud service providers (in particular: AMSB, IT function~~particular AMSB, and the functions responsible for ICT, information security, compliance ~~function~~, risk management ~~function~~ and internal audit);

d. 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;

e. 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

~~c. the oversight of the cloud services including (i) risk assessments~~ and due diligence on cloud service providers, including ~~their~~the frequency of the risk assessment; (ii) monitoring and management controls (~~e.g.~~for example, verification of the service level agreement); (iii) security standards and controls;

d. ~~contractual requirements for material and non-material cloud outsourcing arrangements;~~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; ~~and~~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

~~f. documented strategies to exit ('exit strategies') material outsourcing and to terminate ('termination processes') the cloud outsourcing arrangements regardless of their materiality.~~

~~Questions to stakeholders~~

~~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~~?~~ arrangement.

Guideline 4 - Written notification to the supervisory authority

~~17.~~21. 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.~~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,~~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~~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. 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~~, where applicable,~~ that make use of the cloud services;

c. 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;~~ 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

~~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;~~

~~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);~~

~~Questions to stakeholders~~

~~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?~~

~~Guideline 5 – Documentation requirements~~

~~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,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-outsourcerscontractors 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. and processed;outcome of the assessment of g. whether the cloud service provider (or any significant sub-outsourcer(s))'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;

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 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.

i. a description of the undertaking monitoring of the cloud outsourced activities (i.e. number of resources and their skills).

Questions to stakeholders

Q7. Would the introduction of a register of all cloud outsourcing arrangement have a significant impact on the current undertakings practices to manage cloudoutsourcing 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?

Guideline 6 – Pre-outsourcing analysis

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

a. assess if the cloud outsourcing arrangement is material;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; and 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 – Materiality assessmentAssessment of critical or important operational functions and activities 28.

~~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.~~ 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

~~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)[12].~~

~~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~~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 ~~the conditions of their authorization, and other obligations under the Solvency II Directive~~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, ~~information and communication technology (ICT), cyber~~ICT and legal risks;

   v. reputational ~~and strategic risks;~~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 relevant 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;~~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 ~~undertaking's~~ business area;

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~~f

~~h~~. 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 ~~on the undertaking, policyholders or other relevant subjects including but not limited~~ based on inter alia~~to compliance wit~~h Regulation (EU) ~~2016/679[13]~~2016/67912.. The

undertaking should particularly take into consideration data that is business sensitive and/or critical (e.g. policyholders' health data).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).

Questions to stakeholders

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

Guideline 8 – Risk assessment of cloud outsourcing

28. The30. In general, 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.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

29. Moreover, within their risk assessment in case of material cloud outsourcing, the undertaking should alsoa. 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 weighincluding 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.

30. Carrying out the risk assessment, the undertaking should, at a minimum:b. assess, where applicable and appropriate, the risks, including legal, ICT, compliance and reputational risks, and the oversight limitations

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: i. the selected cloud service (i.e. IaaS/PaaS/SaaS) andand the proposed deployment models (i.e. public/private/hybrid/community);

d. where applicable, assess the risks arising fromii. the migration and/or the implementation;

e. conduct a thorough risk-based analysis of the functionsiii. the activities 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 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 or processed;. The assessment should consider: 1. v. vi. 32.

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;

g. consider the political stability and security situation of the jurisdictions in question, including:

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

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 ofregard to 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-outsourcercontractor is located in a third country or a different country from the cloud service provider;

ii.and the risk that long and complex chains of sub-outsourcing reduce the ability of the undertaking to oversee its material functioncritical or important operational functions or activities 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.the undertakings overall concentration risk to the same cloud service provider

i. assess the concentration risk, including from:

i. outsourcing to a dominant cloud service provider that is not easily substitutable; andor

ii. multiple outsourcing arrangements with the same cloud service provider or closely connected service providers;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. assessment should be performed before entering into a cloud 2. 3. The risk outsourcing. If

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/or significant changes of the services provided or to the situation of the cloud service provider, the risk assessment should be promptly reviewed or re-performed.

Questions to stakeholdersIn 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.

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

Guideline 9 – Due diligence on cloud service provider

32. Undertakings should perform a due diligence on33. The undertaking should ensure in its selection and assessment process that the cloud service provider applyingis suitable according to the criteria defined by theirits written outsourcing policy.

33.34. 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 performedon 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

34.36. 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.

35. In additio37. Without prejudicen to the set of requirements defined by 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 athen undertaking and thea cloud service provider for arrangements classified as material should set out at leastt:

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

b. the start date and, as end date, where applicable, of the next contract renewal date, the end date and/or 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 including the cloud services pricing model;e. whether the sub-outsourcing of a critical or important operational function or activity (or material parts thereof)

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 significant sub-outsourcing is subject to (see Guideline 13);

g. the location(s) (i.e. regions or countries) where relevant data will be keptstored 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 the 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-goingregular basis taking into account the Guideline 14; i

j. the agreed service levels which should include precise quantitative and qualitative performance targets, that are directly measurable by the undertaking in order to independently monitor the services received and, eventually, adopt corrective actionin order to allow for timely monitoring so that appropriate corrective actions can be taken without undue delay if agreed service levels are not met;

k. the reporting obligations of the cloud service provider to the undertaking, including, as appropriate, the obligations to submit the 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

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;
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.

36. Regarding an outsourcing agreement for material cloud outsourcing, 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. Guideline 11 – Access and audit rights 38. The cloud outsourcing agreement should not limit the undertaking's effective exercise of

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).

Question to stakeholders

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?

Guideline 11 – Access and audit rights

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 risks associated with cloud outsourcing arrangements.39.

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. 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,

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.

43.41. If the performance of auditsexercise of its access or audit rights, 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.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.

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), or pooled audit performed by third clients or by a third party appointed by them.

45. Undertakings43. In case of cloud outsourcing of critical or important operational functions or activities, undertakings should make use of the method referred to in paragraph 44(a)42(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.for example, processes, applications, infrastructure, data centres, etc.) and the key controls identified by the undertaking andassesses the compliance with relevant regulatory requirements;

c. thoroughly assess the content of new certifications or audit reports on an ongoingregular basis and verify that the reports or certifications or reports 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.~~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);

f. 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;

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~~g

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

~~46.~~44. For ~~material cloud outsourcing~~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 ~~44(a)~~42(a) are adequate and sufficient to comply with ~~their~~its regulatory obligations ~~but~~and, on a risk based approach, should not rely solely on these reports and certificates over time.

~~47.~~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 ~~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. 46.

~~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~~the relevant audits and/or assessments.

~~Question to stakeholders~~

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

Guideline 12 – Security of data and systems

~~49.~~47. The undertaking should ensure that cloud service providers comply with ~~appropriate IT security and data protection standards.~~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 ~~data and systems~~specific information security requirements in the outsourcing agreement and monitor compliance with these requirements on an ~~ongoing~~regular basis.

~~50.~~49. 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:~~ 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

~~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~~consider specific measures where necessary for data in transit, data in memory and data at rest, ~~such as~~for example, the use of encryption technologies in combination with an appropriate key 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;

c.e. contractually ensure that network traffic availability and expected capacity are guaranteedmeet strong continuity requirements, 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;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

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

g. monitor the level of fulfilment of the requirements relating to the effectiveness and 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.

Question to stakeholdersGuideline 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

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

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 relevant obligations existing between the undertaking andof 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.; c.

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 responsibilityaccountability and oversight obligations for the services it has sub-outsourced.d.

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-outsourcerscontractors or the sub-outsourced services that might affect the ability of the service provider to meet its responsibilitiesobligations 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 casee. 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 should havehas the powerright to object to such changes and/or the right to terminate and exit the contract.

Guideline 14 – Monitoring and oversight of cloud outsourcing arrangements

56.51. The undertaking should monitor, on a regular basis, the performance of activities, the security measures and the adherence to the agreements ofagreed service level by their cloud service 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: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.

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

60.55. In addition to the requirements set out in the Delegated Regulationcase of cloud outsourcing of critical or important operational functions or activities, 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, anthe undertaking should:

a. develop exit plans that are comprehensive, service based, documented and sufficiently tested where appropriate(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, wher and develope 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 an,d 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 irrevocablysecurely deleted by the cloud service provider. in all regions. 56.

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.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; and

e. define success criteria of the transition.

Guideline 16 – Supervision of cloud outsourcing arrangements by supervisory authorities

62.57. The supervisory authorities should perform 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. 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.

63. Supervisory authorities should includeconsider the following risks in the supervision of undertakings' cloud outsourcing arrangements in the context of the followinga. ICT risks:

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

b. IT risks;

c. reputational risk; and

d. strategic risk.concentration risk, including at country/sectoral level. 59.

64. Within their assessments, supervisory authorities should assessinclude 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.. 60.

65. In case of groups, the group supervisor should ensure that the impacts of material cloud outsourcing[14]outsourcing of critical or important operational functions or activities are reflected intoin the group supervisory risk assessment taking into account the requirements listed at the previous twoin paragraphs 58-59 and the group specific's individual governance and operational characteristics. In light of the above, in the context of material cloud outsourcing that61. If cloud outsourcing of critical or important operational functions or activities 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.for example, 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[15].to the group risk profile in the College of Supervisors. 62.

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).

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~~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 ~~the~~ supervision and enforcement of regulatory requirements ~~cannot~~could not be ensured by other measures.

Compliance and reporting rules

~~68.~~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.

~~69.~~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.

~~70.~~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.

~~[14] The materiality of cloud outsourcing is established according to the provisions described in Guideline 7.~~66.

~~[15] As defined in Article 212(1) sub (e) of Directive 2009/138/EC.~~

~~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

~~72.~~67. The present Guidelines will be subject to a review by EIOPA.

~~Question to stakeholders~~

~~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.~~