EUROPEAN FINANCIAL CONGRESS

Instytut Badań
nad Gospodarką Rynkową
Do Studzienki Str. 63
80-227 Gdańsk, Poland

tel. +48 58 524 49 01
fax. +48 58 524 49 09

efc@ibngr.pl
www.efcongress.com

Answers of the European Financial Congress[1] in relation to the European Insurance and Occupational Pensions Authority's Consultation Paper on Guidelines on outsourcing to cloud service providers[2]

Methodology for preparing the answers

The answers were prepared in the following stages:

Stage 1

A group of experts from the Polish financial sector were invited to participate in the survey. They received selected extracts of the EIOPA's consultation document and the consultation questions translated into Polish. The experts were guaranteed anonymity.

Stage 2

Responses were obtained from experts representing:

- insurance firms,
- IT firms
- law firms,
- consulting firms,
- regulators.

Stage 3

The survey project coordinators from the European Financial Congress prepared a draft synthesis of opinions submitted by the experts. The draft synthesis was sent to the experts participating in the survey with the request to mark the passages that should be modified in the final position and to propose modifications and additions as well as marking the passages they did not agree with.

Stage 4

On the basis of the responses received, the final version of the European Financial Congress' answers was prepared.

[1] European Financial Congress (EFC – www.efcongress.com). The EFC is a think tank whose purpose is to promote debate on how to ensure the financial security and sustainable development of the European Union and Poland.

[2] https://eiopa.europa.eu/Publications/Consultations/2019-07-01%20ConsultationDraftGuidelinesOutsourcingCloudServiceProviders.pdf

Answers of the European Financial Congress to the consultation questions

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

The scope of application of the Guidelines should be extended to include an additional category of 'insourcing' or an extension of private cloud to cover an insurance group, that is to say, a service model followed by group companies – for this case, the Guidelines should be adjusted accordingly. Additionally, Community Cloud should be reflected in initiatives between specific participants of the insurance market (e.g. in Poland it would be the National Cloud Operator, the Polish Chamber of Insurance or the Insurance Guarantee Fund). Community is not identified unambiguously.

The scope of application as well as the legal basis and sources of law in the light of which the Guidelines should be interpreted are clear and exhaustive, referring to both hard law and soft law sources (other related EIOPA Guidelines).

With respect to the application of the Guidelines by groups, there are concerns as to the extent to which such provisions are enforceable against non-EU groups which are supervised by local authorities and not an EU-based supervisory authority. For these entities, the Guidelines should limit the applicability of the principle of proportionality (whose correct application is examined by an EU-based supervisor) or even turn more towards a rule-based approach. However, in the case of EU entities which are members of non-European groups, the Guidelines should not restrict the autonomy of their respective EU-based supervisory authorities.

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

The issue of definitions is a fundamental weakness of the Guidelines under review. The Guidelines do not define/explain the concept of outsourcing properly, neither do they define what outsourcing to cloud service providers means, using this name to refer to any activity involving the use of the cloud technology. On the other hand, the definition of a service outsourced to cloud service providers should be based primarily on the answer to the question what kind of service is outsourced, instead of defining the problem solely in respect of the technology used.

Alternatively, Community Cloud could be used in initiatives between insurance companies or market initiatives undertaken by multiple insurers on the market (pooling), e.g. a sales support product only for Warsaw-based companies, motorcycle sales, workshop support etc. The Guidelines do not explicitly prohibit that.

The introduction and definition of the conceptual framework deserve credit. The definition of 'Cloud service providers' may give rise to certain concerns, as while it is indicated that 'Cloud service providers' are entities providing cloud services, it is also stated (in the same definition) that service providers which rely significantly on cloud infrastructure to deliver their services are also covered by the Guidelines. It seems that for the sake of being more specific, it could be indicated that such entities are considered as 'Cloud service providers' for the purpose of the Guidelines.

The term 'material outsourcing', on the other hand, corresponds to the definition of 'Outsourcing of critical or important functions' (Solvency II, Commission Delegated Regulation 2015/35 of 10 October 2014) and 'outsourcing of insurance or reinsurance activities and management system functions' from the Polish Act on Insurance and Reinsurance Activity.

Therefore, it seems that the introduction of 'material outsourcing' as a new term is unnecessary and instead of resulting in understanding, it may lead to more confusion and interpretation difficulties at the company data level (especially for individuals who do not deal with 'regulated' outsourcing on a daily basis).

Definitions of the private, public, community and hybrid clouds refer to an undefined term 'cloud infrastructure' (instead of the defined concept of 'cloud services'), which may raise interpretation concerns.

Furthermore:

1) The definition of 'Significant sub-outsourcer' does not provide for the existence of a chain of significant subcontractors (sub-outsourcers).
2) Instead of the definition of 'Cloud services' in the Guidelines, it would be advisable to use the definition provided in the NIS Directive, in order to avoid situations where a service is understood as a cloud service according to the Guidelines but not according to the NIS Directive (or vice versa).
3) We suggest the use of the term 'distinct types of cloud infrastructure' in the definition of 'Hybrid cloud'.

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?

The answer to this question most likely depends on the individual assessment of the insurance companies covered by this regulation, and in particular on the number and business importance of cloud solutions employed by these insurance companies. If no cloud solutions are currently in use, the proposed timeline does not pose a major challenge to the respondent, because the transition timeline regarding the adjustment to the Guidelines depends on the principal. The timeline may present a higher risk to insurance companies which rely heavily on cloud solutions, in particular with respect to core systems, if their current contracts with outsourcing providers do not meet the requirements of the Guidelines. The proposed content of the Guidelines is relatively difficult to implement if the cloud technology is already used by the insurance company. It will undoubtedly require substantial efforts and necessitate renegotiations of existing contracts with clients.

The implementation of the Guidelines for non-core activities may result in the discontinuation of the technology due to considerable administrative restrictions generating a significant cost increase and compliance risks.

It seems, however, that since outsourcing to cloud service providers is not a new concept for the Polish financial market (including insurance), and the scope of topics covered by the Guidelines largely overlaps the topics and solutions addressed in the Communication from the Polish Financial Supervision Authority of 23 October 2017 concerning the use of data processing in

cloud computing by supervised entities, the timeline for the implementation of the Guidelines should be regarded as appropriate.

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?

The definition of outsourcing set out in Article 13(28) of the Directive is not in itself clear as it can be literally interpreted to mean that it refers to any type of contract under which a third party performs a process, a service or an activity which would otherwise be performed by the insurance or reinsurance undertaking itself. A similar problem exists in banking regulations. Obviously, such a broad interpretation distorts the sense of outsourcing understood as the transfer of a process to a third party and having it managed in such a way that the insurance company itself does not have any resources left to take the process back immediately. Paragraph 10 in Guideline 1 does not modify the broad scope of the definition in Article 13, and only exacerbates the interpretation problems instead. For instance, it points not only to the permanent nature of outsourcing, but also to situations where despite having been outsourced, an activity can be carried out by the insurance company itself, and therefore its wording in a way challenges the nature of 'pulling out' the process.

A further issue is the term 'function' used in the Guideline, having a certain meaning according to the Solvency II system – which may cause further interpretation problems. It is unclear whether the authors meant function as defined in Article 19(29) or any potential outsourced activity.

Solvency II in Article 13(28) defines as outsourcing an arrangement of any form between an insurance company and a service provider, by which that service provider performs a process, a service or an activity, which would otherwise be performed by the insurance company itself. This provision is clear and unambiguous, but please note that a different, lower risk value should be assigned to an outsourcing service provider which is a wholly-owned subsidiary of the insurance company or its group.

Importantly, a particularly valuable feature of Guideline 1 is that outsourcing should be assumed whenever an activity is delivered by a third party. Concerns as to the distinction between cloud services defined as outsourcing and those that do not qualify as outsourcing arise in the context of the conclusions presented in the EIOPA Final Report after consultations No. 13/008 concerning the draft Guidelines on the system of management, paragraph 5.174, which provides examples of activities that should be classified as 'critical or important'.

It follows from that report that a cloud service, if it involves data storage or has an effect on the performance of IT systems, should be qualified as a critical and important activity, and therefore it is considered as outsourcing if it is carried out by a third party, as it is difficult to imagine a cloud service that would not be related to the above areas. For the sake of clarity of the Guidelines, it would therefore be desirable, as in the case of the EBA Guidelines, to specify a list of activities which institutions should not consider as outsourced activities when they are transferred to third parties.

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?

The proposed solutions seem to significantly extend the existing internal outsourcing regulations and reinforce the standards of oversight for outsourced activities. An example of this is the development, aside from emergency plans, of written exit strategies including detailed process timelines, or indication of the need to include outsourcing as an element of the ORSA process – therefore, it will be mandatory even if the insurance company does not consider this risk as significant from the perspective of its operations. This approach gives rise to further difficulties involving the necessary risk quantification in the ORSA process, as it seems that the outsourcing risk qualifies as an operational risk, and operational risks are measured in a simplified manner using the standard formula. The assessment of the adequacy of the standard formula in this context will be practically impossible, for instance due to the fact that insurance companies lack data on the materialisation of this type of risk.

No minimum management standard for outsourced IT services / outsourced service maturity level has been defined – e.g. CMMI, Cloud Computing Governance (TOGAF, COBIT (or Val IT/Risk ITScorecard), ITIL, SOA, ISO 38500), the above standards and good practices address the business needs and IT management. For outsourcing and the highly sensitive area of cloud services, the reference to a standard and its adoption into the Guidelines seems to be very appropriate.

Furthermore:

1) In paragraph 13, it would be advisable to reflect the risk of unexpected and sudden termination of a contract with a provider;
2) In paragraph 15, the security strategy and operational risk management strategy could be added next to the IT strategy;
3) In paragraph 16 (a), the security function could be included;
4) In paragraph 16 (c), it would be a good idea to make a direct reference to ISO 27017/27018 standards.

It would also be appropriate to stress the need to update not only the outsourcing policy but also the security policy – in particular to reflect the 'Shared responsibility model' (where the provider is responsible for cloud security, and the user is responsible for the security of their own cloud resources). This also applies to ensuring that persons responsible for the administration of the contract with the cloud provider and the use of cloud resources and systems (such as IT or security functions) are properly trained and have the appropriate knowledge and competences.

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?

The scope of information is very broad. It seems that in view of the technologies used, it may be very difficult or impossible to answer some questions in an unambiguous way, such as the location of specific data. It should be noted here that Guideline 4 does not cover all information

submitted to a supervisory authority, as it does not take into account the information provided as part of ORSA or SFCR reports.

The Polish supervisory authority already requires a lot of very detailed information with respect to reporting on outsourcing of critical and important activities, and therefore the scope of reporting set out in Guideline 4 does not seem to introduce a significant change in this respect. In some cases, reporting under subparagraph (e) could prove difficult, as detailed information on corporate structures and groups of companies will not always be readily available, especially in the case of providers which are members of large international groups.

In subparagraph (f), the description of provider's activities should be clearly and precisely limited to the area related to the outsourced process only, in order to avoid the need to describe the full range of activities carried out by a potential provider who may operate across multiple industries.

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?

In our opinion, the introduction of a register of all outsourcing contracts into the cloud will not have a significant impact on the current practices of undertakings in this area. Institutions keep records of outsourcing contracts in accordance with the Polish laws. While the minimum scope of recorded information is narrower than that prescribed by the Guidelines, supplementing it with the data required by the Guidelines should not pose a major organisational challenge for institutions, as most of the information is collected for the purposes of risk analysis or due diligence of the insourcer.

The introduction of a register containing all items specified in the aforementioned Guideline will certainly mean an increased administrative and bureaucratic burden for new market participants with regard to cloud outsourcing contracts. Furthermore, the special treatment afforded to cloud services (regardless of their level of materiality/significance) is not fully clear, especially in relation to outsourcing of other critical and important services. This will undoubtedly significantly compromise the usability and processing flexibility of cloud outsourcing contracts, which could particularly affect services for which there is a particularly urgent demand and/or the actual use of a non-cloud solution is impossible or very difficult.

On the other hand, such detailed reporting methods and tools will probably contribute to facilitating and improving the monitoring of the outsourcing process by insurance companies.

The register of outsourcing contracts is already in use, so it will not have a significant impact, provided that the register can still be kept in any format (such as Excel, Access, or other IT tools).

Q8. Are the documentation requirements appropriate and sufficiently clear?

The requirements are clear but too broad (audits, risk assessment, a description of the monitoring of a given service provider). The scope of requirements appears to be formulated in an unambiguous manner. However, coupled with the nature of outsourced and cloud services, it

may give rise to interpretation problems. In this context, doubts arise as to the nature of outsourced services – do they include the possibility of using software, technical support for software used or, for example, data storage or calculation capabilities – which of them qualify as outsourcing (outsourced services), what is the nature of risk, how it will be defined and estimated, and how the service itself should be supervised.

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?

It is appropriate, but not clear enough. However, the defect does not lie in the Guidelines (which define the concept of 'materiality'), but in the underlying regulations, which define the concept of 'critical or important operational function'. Paragraph 60 (EIOPA Guidelines on System of Governance) is formulated in a way that makes it actually possible to qualify EVERY activity carried out within an undertaking as a critical or important activity. If every activity is (or can be) qualified as 'important', any (however advisable) attempts to use a 'materiality' filter at the level of the Guidelines are therefore doomed to fail. Without any minimum conditions, materiality is rated too high as a parameter to serve as an objective judgment and standard. There is a very high risk that materiality assessments will differ considerably depending on the market player.

For example, if we discuss a basic system supporting a critical process for an insurance company, outsourcing to a cloud can be assessed with a low level of materiality, since insurance contracts exist in paper form and it is possible to recreate the process and provide the client with an adequate and timely resolution of the claim – and therefore a basic system that is critical to business continuity becomes an auxiliary system that 'digitises' the workflow. The Guidelines should additionally include a process to update the materiality assessment.
Furthermore:

1) Paragraph 27 states that in order to determine the materiality of a service, aside from risk assessment, a range of factors should be included whose examination would constitute risk assessment in itself;
2) Paragraph 27 (e) should be made more specific, for example by replacing the term 'cost of the cloud outsourcing' with 'annual contract value' or a similar term;
3) In paragraph 27 (h), it could be advisable to make a reference to the Data Protection Impact Assessment process required by the GDPR.
4) The idea of risk insurance (27 (f)) seems to be risky – while it may offer protection against material losses, it could prove detrimental to companies in the long run if business cannot be recovered after prolonged downtime.
5) The process of materiality verification should be carried out at least once a year, and a disaster recovery process should be provided for particularly critical cloud-based business systems/functions in another geography of the same provider, by another provider or, as a last resort, on-premise (as briefly specified in paragraphs 27g and h).

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

The solutions presented do not seem to raise any concerns. Risk assessment considerations are presented in a concise yet complete manner that captures their substance. The risk assessment presented in the Guidelines is embedded in the risk-based approach concept and is conducted in proportion to the size and business scale of an institution.

The assessment of the risk of long and complex chains of sub-outsourcers ruling out or reducing the ability to ensure proper oversight of activities seems to be a complex process with an uncertain outcome and therefore this type of risk should be subject to mitigation (approach based on statutory law is preferred).

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

The requirements are clear; however, some of them are difficult to meet for objective reasons, such as setting out the location where data will be processed. Given the common use of distributed data centers, a service provider itself may not be aware which 'machine' supports a given entity at a given point in time, and the locations are so plentiful that listing them all would not produce the expected supervisory outcome. It seems that the question should be whether the entity performs the contract in accordance with the agreed rules and the laws applicable to the insurance company, and not where the contract is actually performed. Jurisdiction over the contract itself and over the registered office of the entity is important, and so is the performance security, if any.

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

These requirements in fact refer to a rather general criterion of the type of data outsourced to a cloud. Perhaps the examples prepared by EIOPA have contributed to a better understanding of what contractual requirements should be included in the contract depending on the data type. On the other hand, it is difficult to imagine that outsourcing contracts involving significant amounts of data, production data or sensitive data would not be considered material/important. In our view, in practice this wording used in the Guideline is likely to mean that insurance companies will need to take a conservative approach and seek/endeavour to include all the requirements of Guideline 10 in their cloud outsourcing contracts, regardless of the materiality level.

Furthermore:

1) In paragraph 35, it should be ensured – perhaps by adding more detail to subparagraph (e) – that information on incidents (at least those critical) is provided to the insurance company. The insurance company should also be informed of any planned unavailability.
2) In paragraph 35 (h), it would be useful either to define individual attributes or to refer to attributes defined in ISO2700X or the NIS Directive in order to avoid confusion of terms.
3) In paragraph 35 (m), it would be useful to add the obligation to inform the insurance company about testing results.

4) Paragraph 50 fails to cover several issues which surface as security weaknesses in the practical application of clouds within organisations, due to the inadequacy of policies, technologies and knowledge relevant to on-premise security management. These issues involve:
   a) Security monitoring relevant to the cloud-based service model;
   b) Understanding of security mechanisms offered by a cloud service provider and their proper application, in particular with regard to secure service setup;
   c) Definition of security requirements (procedural and architectural) relevant to cloud services and reflecting them in the pre-service on-boarding and validation process;
   d) Clear separation of responsibilities and a cooperation model in case of actual or suspected security incidents (with predefined response times).
5) Planning and following a training process to maintain an appropriate level of knowledge (which could be demonstrated by technical certificates).

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

It could be difficult for institutions to exercise such broad rights of access and auditing. Auditing of sub-outsourcers could pose a particular challenge, especially in the case of very complex outsourcing chains. Making equipment available to institutions or other designated entities may result in a breach of the supplier's business secrets, or even professional secrecy.

It should be assumed that most organisations will not conduct their own provider audits and will instead rely on reports from auditors such as SOC – Service Organization Controls, ISAE3402, etc. It would be appropriate for the Guidelines to include provisions concerning the frequency of obtaining such reports, analysing the auditor's opinion, adjusting the provider's objectives and controls to the organisation's internal control environment and risk management system, analysing the impact of reservations to the auditor's opinion and/or identified exceptions and questions, and ensuring that the user-organisation controls mentioned in the auditor's report have been implemented and are effective.

Furthermore:

1) If SSAE18 is sufficient in respect of meeting the expectations of paragraph 45, it would be useful to state this directly, and otherwise it would be appropriate to indicate what should be added to the report.
2) Paragraph 46 should indicate what else insurance companies should rely on (even by way of example). We also suggest that audit firms should be rotated (e.g. in a 5-year cycle).

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

For many individual insurance companies, Guideline 12 will be in many respects difficult to follow. This applies in particular to the control of actual cloud data management, which requires specialist knowledge and access to the technological solutions of the cloud service provider. The decision to use a cloud is often dictated by insufficient qualified in-house resources to maintain high security standards. In the light of the above, an acceptable solution

would be to adopt the same principles as in Guideline 11, i.e. to include certificates and third party audits and to monitor the design of the security management system itself.

Monitoring of provider vulnerability management by insurance companies is not addressed. We also suggest that penetration testing should be referenced directly as the expected approach to verification of the material security level of outsourcing.

It would also be appropriate to reflect the 'Shared responsibility model' (where the provider is responsible for cloud security, and the user is responsible for the security of their own cloud resources).

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.

The Guidelines do not follow the principle of proportionality, as the proposed outsourcing approach covers all activities of an insurance company, regardless of their materiality. The materiality criteria applied do not relate to the essence of outsourcing, instead they are based on the cost of the contract and the risks generated.

Outsourcing is not an end in itself, but an entity's response to its actual capabilities and the risk mitigation method. In addition, a distinction needs to be made between outsourcing and mandate, software purchase, consulting, support or other types of contracts with third parties. Outsourcing means subcontracting an organisation out a process which is not or will not be supported internally, because the Company cannot or does not want to maintain it, perhaps due to significant costs of the process.

For instance, outsourcing should not include: using a cloud-based office suite, which is purchased software and, as a rule, is supported by a third party (similarly to a car that is serviced under warranty by an authorised provider but no one would claim that the purchase of a car and its servicing classify as outsourcing, because in theory it could be manufactured and serviced for the organisation on an individual basis, incurring a certain level of expenditure). By analogy, use of database space would not be considered as outsourcing either, as no one regards the manufacture or purchase of portable hard drives on which data resources can be stored as outsourcing. On the other hand, it would be considered as outsourcing if an end-to-end process is transferred to a cloud, such as fully independent management of the system administration process or full assignment of services relating to a specific IT system (from development to implementation, administration, to the introduction of production changes for corporate purposes). Further to that, the said definition of outsourcing would not require the assessment of service materiality, as subcontracting out the entire process of company functioning is material by nature.

However, the above approach does not hinder the management of the risks arising from external contracts. These risks should be managed (but not as an outsourcing risk), for example data security guaranteed in databases (just like data security on a portable drive), but the nature of the risk is different and it is analysed under a contract. In the first case, data availability, security and integrity are important for the undertaking, while in the second case it is the ability

to run a business process in view of a lack of internal resources. Therefore, risk mitigation methods will be different. In the first case, these will be data backups, and in the second case – ensuring a smooth transition between the teams supporting the process (regardless of their location).

To sum up, the Guidelines should be preceded by defining exactly when the outsourcing service occurs and, additionally, a separate subset should indicate in which cases a cloud service is an outsourcing service.

Furthermore:

1) In paragraph 56 (e), the purpose of distinguishing between IT security and cybersecurity is not clear. Additionally, the expectation for a clear separation of IT and non-IT processes expressed in this section will not always be possible (for example where insurance products are sold by electronic means);
2) In paragraph 60 (a), it is not clear in which cases the testing is actually expected;
3) If operational risk in the insurance sector is to be defined in the same way as it is in the banking sector, then IT risk should be included in the operational risk framework;
4) In addition, we suggest the introduction of a mechanism for cooperation and knowledge sharing between supervisory authorities to ensure a uniform supervisory approach and a level playing field;
5) Paragraph 60 (b) refers to the identification of alternative solutions. For important and critical systems, solutions enabling easy change of provider (multi-cloud), which do not consume significant effort or time, should be preferred instead (to avoid a 'vendor lock').

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

Impact Assessment is extremely useful as an introductory document. It perfectly shows the alternatives available to the authors of the Guidelines and contributes to understanding why the options which are now the 'backbone' of the document under development have been finally chosen.

However, in the Impact Assessment, EIOPA actually did not describe any quantifiable impacts of the introduction of the Guidelines on insurance activities and the IT services industry. Reference was only made to potential compliance risks due to differing definitions of the same problems by national supervisors. Market benefits, on the other hand, are defined only in the framework of harmonisation of standards.

The document does not indicate that the regulation itself would generate transposition costs, as a minimum. Significant regulatory risks which should be mentioned here include inhibiting the development of the cloud technology in the financial sector, as it may turn out too expensive and too risky for insurance companies to implement in their operations. At the same time, the proposed legislative solutions do not address the main problems involved in the business of insurance companies, including personal data protection, limited highly qualified IT resources, flexibility of IT solutions or access to services powered by mobile technologies.

General comments

i. The document does not clearly specify who will play the supervisory role – a regulatory authority, or perhaps the insurance company itself? Moreover, the Guidelines do not place enough emphasis on the outsourcer's liability for principal's/client's losses caused by improper performance or non-performance of contracts. In the event of a failure or other significant malfunction, it is the outsourcer who has to initiate an action plan in the first place. The outsourcer should be required to have a disaster recovery centre. If its plan fails or turns out sufficient, the principal will need to implement its plan. Reversal of the process, in which case the principal's plan would be followed, would discourage the outsourcer, and as a result the risk would increase and would be fully passed on to the principal.

ii. The Guidelines set very high expectations for insurance undertakings regarding controls, scope of documentation and roles which will be necessary to meet the requirements both at the stage of preparing the cloud adoption strategy and at the stage of cloud management. All these activities may imply additional operating costs for insurance companies, mainly related to staff training and maintenance of the existing processes.

As a result, the EIOPA Guidelines may additionally hinder cloud adoption in the insurance sector. In the light of the above, we therefore encourage further consultations, which should result in the emergence of a practical regulation.