|  |  |
| --- | --- |
| Date : 27 09 2019 | |
| N° Registre de transparence 5149794935-37 | |
|  | |
| Objet : | Consultation paper on the proposal for Guidelines on outsourcing to cloud services providers |
|  | |

# commentaires de la fédération française de l’assurance (FFA)

## General comments

The FFA studied carefully the EIOPA consultation paper on the proposal for Guidelines on outsourcing to cloud service providers. The FFA thanks EIOPA for giving the possibility to comment on this proposal that really got our attention.

First of all, regarding outsourcing and data protection, the FFA would like to precise that insurance companies have already to comply with very complete sets of rules which must remain the references (see for outsourcing: Solvency 2 regulation and for data protection: GDPR regulation).

**We believe that all relevant texts regarding outsourcing or data protection should refer to Solvency 2 or GDPR and their terminology.**

Having said that, proposing a formal framework regarding the specific issue of cloud outsourcing could be useful; there is an interest in formulating a specific approach to this technology which is becoming increasingly important for all areas of activities. Indeed, for insurance sector, giving clarification and transparency to market participants regarding cloud outsourcing arrangements could be useful.

We believe that, at this point, the proposed approach seems difficult to consider taking into account:

* the lack of proportionality and the systematic nature of the proposals, Cf; 1/
* the introduction of a new concept: “material outsourcing” which does not exist into Solvency regulation, Cf. 2/
* excessive burdens for insurance companies regarding contractual requirements, audit and control on cloud service providers, Cf. 3/
* a too short timeline, Cf. 4/
* insurance group specificities which are not taken into account, Cf.5/

Furthermore, the FFA does not understand why the proposed guidelines are much more detailed than EBA guidelines.

Regarding the form and the general presentation of the document, it is difficult to understand which guidelines are only applicable to material cloud outsourcing arrangements and guidelines which are also applicable to non material cloud outsourcing arrangements.

In this context, we would like to suggest a couple of key points to make EIOPA’s proposals operational in order to facilitate relationships between insurers and cloud service providers.

1/ Lack of proportionality/systematic nature of the proposals

First of all, the FFA would like to recall that, regarding outsourcing arrangements, the insurance sector has to comply with a very detailed and complete set of rules[[1]](#footnote-1). Furthermore, the FFA would like to precise that the use of cloud outsourcing is steadily increasing and involves in many cases non critical or important business activities of the insurance company. Obligations contained in the guidelines regarding, documentation requirements, pre-outsourcing analysis, due diligence…concern all cloud outsourcing and involve disproportionate means, costs and extended deadlines.

Therefore, the FFA believes that EIOPA should adopt a proportionated approach regarding cloud outsourcing arrangements which are not directly relevant to critical or important functions or activities (see solvency 2 regulation); **the scope of the guidelines should be reviewed in order to exclude cloud outsourcing arrangements which are not directly relevant to critical or important functions or activities of the insurance company.**

Furthermore, intra-group outsourcing should be taken into account: there are indeed fewer risks in this type of intra-group transactions and the principle of proportionality should encourage the introduction of lighter requirements (monitoring, pre-analysis, audit, exit clauses and documentation…).

2/ Introduction of a new concept: “material outsourcing”

The introduction of a new, unclear term: “material outsourcing” adds a level of complexity and confusion.

Indeed, Solvency II regulation (Directive 2009/138, delegated regulation 2015/35, EIOPA guidelines on system of gouvernance-section11) only refers to “critical or important operational functions and activities”.

EIOPA should use existing terms and concept in order to avoid any confusion or source of misunderstanding. The proposed Guidelines should refer to Solvency 2 regulation and delete the very confusing notion of “materiality”.

**These guidelines should just focus on a “translation” or an interpretation of existing requirements (Solvency II Corpus regarding outsourcing) to a limited number of special aspects and issues related to cloud computing.**

We believe that cloud outsourcing is “only” another form of outsourcing and therefore should follow the same logic as “traditional” outsourcing (as referenced in Solvency 2).

There is no reason to develop for cloud outsourcing arrangements more stringent rules than for other outsourcing arrangements.

3/ Excessive burdens for insurance companies regarding contractual requirements, audit and control on cloud service providers

It should be stressed that all of the burden of complying with these guidelines is borne by the insurer (contractual requirements, audit, monitoring and oversight). The FFA would like to stress that, in the context of its contractual relations with giant cloud providers it will be very difficult to impose contractual rules or audit rights.

Therefore:

* **the FFA strongly encourages EIOPA to engage with cloud service providers to ensure their willingness to adhere to all these very heavy requirements.**
* **Regarding contractual relationships with cloud service providers, a solution could be to elaborate, at EU level, model clauses complying with competitions rules.**
* Regarding multiple and disproportionate controls on cloud service providers**,** **it could be appropriate to elaborate an ISO certificate for these providers,** guaranteeing the continued compliance with high level safety requirements with which the insurers and other interested parties can trust.
* If cloud providers where such a critical infrastructure, supervision of these actors could be as well envisaged.

4/ A too short timeline

Insurance companies have complex structures, any change in their systems/process is usually very time consuming.

That is why regarding proposed timeline to implement the guidelines, an additional time period to comply with the requirements should be granted, the proposed dates are too short, even if the FFA welcomes the flexibility proposed if the review of cloud outsourcing arrangements is not finalized by 01 July 2022.

Indeed, these guidelines will involve important contractual renegotiations, therefore the deadline of 1 July 2020 regarding new arrangements, **which are already under negotiation**, is too short for the correct application of final guidelines published in January 2020.

Regarding existing cloud outsourcing arrangements, an additional period should be granted to ensure that could outsourcing arrangements are compliant with the guidelines.

5/ Insurance group specificities which are not taken into account

The French market have a significant number of big actors (8 International Active Groups in the ICS framework); most of them have a holding company acting on behalf of its subsidiary.

EIOPA does not take adequate account insurance groups with a holding acting on behalf of its subsidiaries. This particular issue should be addressed in the proposed guidelines.

## Detailed answers

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

No, please refer to our remarks above.

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

Generally speaking, the FFA does not understand why the number of definitions of EIOPA guidelines is far more important than definitions listed in EBA guidelines. **As a general principle, all the definitions contained into the Guidelines should absolutely refer to those included into Solvency 2 regulation.**

* The definition of “*function*” should be deleted, recital 31 and art. 13.29 of Solvency 2 directive already contains a definition of function[[2]](#footnote-2); the guidelines should only refer to the Solvency 2 definition.
* The definition of “material outsourcing” should be removed or only refers to “*outsourcing of critical or important operational functions or activities as defined in Solvency 2 regulation*”.
* The definition of “*service provider*”: is not clear. What is meant by “*performing an outsourced process, service or activity, or parts thereof, under an outsourcing arrangement*”? Does that include third parties which are not cloud service providers but rely significantly on cloud infrastructure to deliver their services, as well as cloud brokers?
* The definition of “*cloud service provider*” is far too broad and would force insurance companies to take into account all IT service providers. What is meant by third party who “*rely significantly on cloud service providers to deliver their services*”?
* The definition of “*cloud broker*” should be deleted to the extent that the term is not used anymore in the text of the guidelines.
* The definition of “*significant sub-outsourcer*” is not clear, it is too broad.
* The definition of cloud services should insist on the opposition between the cloud and local storage: this kind of definition could be proposed: “*Services provided through a cloud, i. e. a set of computer resources (e. g. networks, servers, storage, applications) that are exclusively accessible remotely and allow computer processing without local storage of data or applications and without the service customer receiving dedicated computer resources*.”
* Public Cloud: this definition should be precised
* Private Cloud: this definition should be precised

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?

No, please refer to our remarks above.

Q 4 Is the Guideline on cloud services and outsourcing appropriate and sufficiently clear to enable the distinction between cloud services falling within the scope of outsourcing and the ones not falling within such scope?

For us, the guideline is quite unclear; examples/clear criteria should be given of what should not be considered as outsourcing to cloud service providers, as many companies providing IT services rely on clouds for their own activity. Indeed, there are many services that should never be expected to be undertaken by an undertaking itself (e.g. emails system, procurement of storage space/server capacity) and can be classified as a mere purchasing of services rather than as actual outsourcing of the same.

|  |
| --- |
| Conclusion: only the functions and activities which are deemed critical and important for the activities of the undertaking under Solvency 2 rules should be covered by the Guidelines and only where actually outsourced to a cloud service provider. |

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?

For the FFA, there is no need to elaborate a guideline regarding written policy which already exists with Solvency 2 requirements regarding outsourcing.

|  |
| --- |
| Conclusion: cloud outsourcing arrangements (related to critical or important function or activity) should be integrated into the overall outsourcing process to ensure a consistent governance. |

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 notification requirement should be limited to cloud outsourcing arrangements involving critical or important function or activity. The list of information to be notified should be in line with notification required by Solvency 2 regulation regarding outsourcing (only for critical or important function or activity). Practical details regarding this notification’s procedure should be decided at national supervisory authority level.

|  |
| --- |
| Conclusion: the notification of a cloud outsourcing agreement to the national supervisory authority should follow the same rules and be in the same form than that provided for any other Solvency 2 outsourcing arrangement. |

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?

For a sound governance, the FFA is not opposed in principle to list cloud outsourcing arrangements regarding critical or important functions but the guideline gives too much details; the form and the location of this kind of information should be taken by the insurance company. Indeed, Insurance companies should have more flexibility with regards to the oversight of cloud outsourcing arrangements.

The FFA would like to stress the difficulty of maintaining and updating a register regarding cloud service arrangements, because of the pace of change regarding cloud outsourcing offers and the number of departments involved in the process.

Furthermore, the FFA does not see the need of a special register for cloud outsourcing arrangements. Cloud out-sourcing arrangements should be mentioned in the general outsourcing register/document.

Finally, the requested documents regarding the description of the services used and the data stored raise confidentiality concerns; communicate these kinds of highly confidential information outside the company presents a real risk.

|  |
| --- |
| Conclusion: there is no need for a special register regarding cloud outsourcing; should there be a requirement for a separate register, insurance companies should be let free to elect the deemed appropriate mean/tool for the oversight of their cloud outsourcing arrangements and it should be limited to cloud outsourcing arrangements relating to critical or important function or activity and the information to be populated in such a register should be limited to what is strictly necessary to ensure monitoring, all other information being in any case duly recorded in the contract itself. |

Q8 Are the documentation requirements appropriate and sufficiently clear?

The documentation/information requirements listed under paragraph 23 appear unnecessarily stringent and burdensome, in particular:

* 23(a) duplicates the notification;
* 23(c) unnecessary, already provided for in the undertaking policy (should be the same for all arrangements entered into by a given undertaking);
* 23(d) interest of having estimate cost in the register unclear;
* 23(f) the mentions regarding sub outsourcers should be incorporated in the contract itself not in a register;
* At paragraph 23(g), please clarify what is meant by “time critical”.
* As regards paragraph 23(i), the required level of detail regarding the description of the undertaking monitoring of the cloud outsourced activities is too specific. Considering that the number of resources and their skills may vary from time to time, it would be too burdensome to regularly update the register in that regard.

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?

No, as explained above, EIOPA should absolutely delete this new confusing concept and stay with Solvency 2 concept regarding important or critical functions or activities.

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

* We understand that Paragraph 28 apply to all cloud outsourcing, 29 only for material outsourcing, what about paragraph 30 ?
* Please provide examples of “high-severity, operational risks events” in the context of cloud outsourcing, as referred to in paragraph 28.
* At paragraph 30(g)(i), “the laws in force” is too broad, there should be limitative list of laws to be taken into account within the risk assessment (e.g. laws on data protection).
* The risk assessment methodology should not so differ, subject to the very specificities of cloud services, from that applicable to the outsourcing of important or critical functions or activities.
* This Guideline should also take into account the impact of events affecting the cloud service provider.

|  |
| --- |
| Conclusion: risk assessment regarding cloud outsourcing arrangements is already covered by the risk assessment conducted as part of the general outsourcing arrangements. For the FFA the proposed list of elements to be verified by the insurance company should be indicative and should not be binding. |

Q11 Are the contractual requirements for material outsourcing appropriate and

sufficiently clear?

Generally speaking, the FFA would like to stress that in most cases, the service provider offers a standardized and packaged offer, which is identical for all its clients, and which can hardly be adapted and customized for a specific client. Furthermore, art. 274 Paragraph 4 delegated act 2015/35 regarding general sub-outsourcing already describes (only for outsourcing of critical or important operational functions or activities) the content of the written agreement between the undertaking and the service provider in exhaustive detail. Nonetheless, Guideline 10 (Paragraph 35) sets out a number of new requirements (“in addition to the set of requirements defined by Article 274…”). We see no benefit in the additional requirements. Finally, to our knowledge, EBA Guidelines do not contain any list of contractual requirements…

* Regarding 35. The use of such terms as “at least” is confusing.
* Regarding 35.d (“*the parties’ financial obligations including the cloud services pricing model*”) could be a problem: currently, major cloud service providers only propose on-line price models; therefore the guidelines should absolutely refer to the price model available on-line.
* 35.i monitoring cloud service provider cannot be “on an ongoing basis”, the term “regular” should be preferred.
* At paragraph 35 j, please provide examples of quantitative and qualitative performance targets that are directly measurable by the undertaking.
* Regarding 35.l of the guidelines (“*whether the cloud service provider should take mandatory insurance against certain risks and, if applicable, the level of insurance cover requested*”) for instance, it is up to the contractual parties to consider insurance coverage for the outsourced activities and whether this issue should be addressed in the outsourcing agreement. This should remain so…
* Regarding 35.n: this provision will be difficult to apply, in case of bankruptcy the treatment of contractual debts and credit depends on legal provisions or on liquidator/court administrator’s decision.

|  |
| --- |
| Conclusion: for all the reasons explained above, the Guideline 10 could be removed. Regarding contractual relationships with cloud service providers, a solution could be to elaborate, at EU level, model clauses complying with competitions rules.  Indeed, insurance undertakings suffer from a weak bargaining power compared to giant cloud service providers, models clauses compulsory for contracting parties could be the solution |

Q12 Are the criteria provided to set the contractual requirements for non-material

outsourcing appropriate and sufficiently clear?

There should be no contractual requirements for non-material cloud outsourcing arrangements, which should not fall within the scope of these Guidelines.

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

Many questions arise from Guideline 11

* Regarding these pooled audits, it is a good idea which must be further explored; however, cumulative requirements in 45 seem difficult to meet.
* Please clarify paragraph 45(a). To which audit plan are you referring to?
* At paragraph 45(b), the use of both “i.e.” and “etc.” makes it unclear whether the list of systems in brackets is limitative or not. Also, it refers to “systems” and “key controls”, while paragraph 45(d) refers to “key systems and controls”. Please correct this inconsistency and clarify the notions of key systems and controls.
* At paragraph 45(c), “thoroughly” should be removed. Paragraph 45(c) should not amount to requiring a thorough audit of audit reports.
* At paragraph 45(d), it is unduly burdensome to require undertakings to ensure that key systems and controls are covered in future versions of the certification or audit report. Undertakings should only ensure that key systems and controls are covered in the scope of the certification or audit report at the time they are using it as an audit method.
* At paragraph 45(e), what is meant by “rotation of the certifying or auditing company”?
* At paragraph 45 (g), difficult to apply, regarding most of cloud outsourcing arrangements, the service provider offers a standardized and packaged offer, which is absolutely identical for all its clients, and which can hardly be adapted and customized for a specific client (including audit aspects).
* At paragraph 45(h), please clarify the extent of on-site audits in the context of cloud outsourcing, bearing in mind that the full rights to access and audit for outsourcing undertakings is difficult to implement in view of highly standardized services and contracts, the limited negotiation power of outsourcing undertakings, the risk these rights pose to the cloud environment of other clients of the cloud service provider, and the risk and operational implications for the cloud service provider as a whole.
* At paragraph 48, please clarify the requirement on “the appropriate skills and knowledge”.
* How to measure satisfaction as referred to in paragraphs 45(a), 45(e) and 45(f)?
* Please clarify that paragraphs 43 to 45 apply to both access and audit rights (not just audit). E.g. paragraph 43 should start with “If the exercise of access or audit rights, or the use of certain audit techniques…”.

|  |
| --- |
| Conclusion: the FFA would like to stress the difficulty of gaining acceptance for these access and audit rights (not least for reasons of confidentiality). In practice, it is common contractual practice for service providers to provide a limitation on the number of audit rights per year: is such as limitation considered an impediment to the rights of access and audit as per paragraph 39?  As said before, cloud service providers could comply with an ISO or SOC (Service Organization Control) certification guaranteeing the continued compliance with high level safety requirements with which the insurers and other interested parties can trust. |

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

Regarding data protection requirements, insurance sector has already to comply with GDPR regulation, which must remain the reference.

Ongoing monitoring appears extremely stringent, or even possible to achieve. Insurance undertakings have already developed a PAS (Plan d’Assurance Qualité) annexed to the cloud agreement.

At 50 (d), such proposal goes too far because of including the sub-outsourcers.

At paragraph 50(g), please clarify how, and at which frequency, the undertaking should monitor the level of fulfillment of the requirements relating to the efficiency of control mechanisms implemented by the cloud service provider and its significant sub-outsourcers. Also, such monitoring should be limited to the cloud service provider as it is the cloud service provider’s responsibility to monitor its sub-outsourcers.

|  |
| --- |
| Conclusion: the FFA is in the opinion that these obligations must be borne by cloud service providers. As said before a solution could be to elaborate an ISO certificate for these providers, guaranteeing the respect of a high level safety requirements regarding security data and systems. |

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.

As a general principle it seems excessive to apply, beyond what is required from the very cloud services specificities, more stringent governance rules to the cloud outsourcing process than those required to be complied with for the outsourcing of key functions.

Undertakings should be given some flexibility in the way they follow-up on and monitor, in compliance with Solvency 2 requirements, their Solvency 2 outsourcing arrangements. In the future a wide range of tools may become available which would render the suggested “register” obsolete. Furthermore, the register proposed in the Guidelines and the information requested to be populated therein appear in practice hardly manageable for the undertakings considering, in particular, the number of contributors the ongoing update of such a register would involve without clear added-value for the undertakings as long as they keep strict record of their arrangements and have tools in place to duly monitor the various aspects of the arrangements in force.

|  |
| --- |
| Conclusion: As explained in our general comments, the guidelines suffer from a lack of proportionality; the best way to ensure proportionality is to restrict the scope of the guidelines to cloud service arrangements regarding critical or important function or activity and stay in line with Solvency 2 requirements regarding outsourcing arrangements. |

GL 13 Sub-outsourcing

For the FFA, it should be a general rule: all sub-outsourcing arrangements are prohibited except those which are explicitly authorized by the insurance company, paragraph 53 should be amended accordingly.

Furthermore, it is impossible for an insurance company to control all sub-outsourcers; the control should be restricted to outsourcer who are contractually bound to the insurance company ; sub-outsourcers must be controlled by the cloud service provider. One possibility could be, for the insurer, to ask for the own outsourcing policy of the cloud service provider.

-----------------

1. See Solvency 2 Directive 2009/138, delegated regulation 2015/35, EIOPA’s Guidelines on system of governance, RGPD 2016/679 [↑](#footnote-ref-1)
2. “*A function is an administrative capacity to undertake particular governance tasks. The identification of a particular function does not prevent the undertaking from freely deciding how to organize that function in practice save where otherwise specified in this Directive. This should not lead to unduly burdensome requirements because account should be taken of the nature, scale and complexity of the operations of the undertaking. It should therefore be possible for those functions to be staffed by own staff, to rely on advice from outside experts or to be outsourced to experts within the limits set by this Directive*.” And “‘function: *within a system of governance, means an internal capacity to undertake practical tasks; a system of governance includes the risk-management function, the compliance function, the internal audit function and the actuarial function*; [↑](#footnote-ref-2)