EIOPA - Consultation Paper on the proposal for Guidelines on outsourcing to cloud services providers.

INTRODUCTION

ABOUT IRISH LIFE GROUP

Canada Life was founded as Canada´s first life insurance company in 1847. It has now grown into one of the world´s largest and most financially secure providers of life insurance. Since 2003, Canada Life has been a part of Great-West Lifeco Inc., one of the leading financial service providers in Canada. Great-West Lifeco Inc. cares for more than 28 million clients around the world.

Canada Life operates in Ireland under both the Irish Life and Canada Life brands. Irish Life Group empowers its customers to look to the future with more confidence and certainty. We manage the financial needs of more than 1.3 million Irish customers. We think ahead to find opportunities and anticipate challenges to help deliver more security and certainty for their futures. We have over 75 years' experience serving corporate and private customers in Ireland. We pride ourselves on having a deep understanding of our customers' needs, interests and concerns for themselves and their families.

Irish Life Group (ILG) includes Irish Life Assurance, Irish Life Health, and Irish Progressive Services International (IPSI) as well as its associated companies Irish Life Investment Managers and Setanta Asset Management. We currently have 2,400 people working at our campuses in Dublin and Dundalkand we continue to grow.

EXECUTIVE SUMMARY

The Irish Life Group welcomes the opportunity to participate in this discussion paper with EIOPA.

The Irish Life Group companies and the Canada Life companies based in Ireland is one of the largest and most diverse financial services groups in Ireland, focussed on providing a wide range of investment, reinsurance, protection and health insurance products to consumers. As such, we actively seek opportunities to ensure better outcomes for our customers through meeting their needs in a cost efficient, flexible and timely manner.

There can be instances where utilising the benefits of a cloud service provider helps us to achieve our objectives without materially impacting on our risk profile, subject to the right controls being in place to address specific cloud risks, including third party risks associated with cloud use. In fact, there is often a strong case to use such services in order to further enhance our products and services. Cloud computing can increase scalability and flexibility in sourcing computing resources, while also potentially introducing security benefits. As a Group we are very aware of the additional risks to which the use of cloud technologies may expose firms and the importance of identifying and managing these risks.

The degree, nature and risk posed by outsourcing can vary extensively depending on the type of cloud used. There are marked differences in the risks associated with IaaS, PaaS and SaaS respectively. Therefore, blanket governance arrangements on all types of cloud may be neither appropriate, proportionate nor ultimately beneficial to the customer. We believe that more detailed

guidance pertaining to the different nature of risks presented by the different cloud usage models would allow for more proportionate response to EIOPA's concerns.

SUBMISSION – Commentary on the Guidelines

Introduction

Irish Life Group firmly agrees with the principle of proportionality as set out in point 3 within the introduction to the Guidelines. It is our view that it is of critical importance that competent authorities across all Member States are aligned with regards to this principle and apply it consistently across all jurisdictions. To allow wide interpretations on proportionality would potentially create regulatory arbitrage and increase complexity across the Internal Market.

Some criteria that could be considered in assessing the proportionality of each arrangement would be:

- The materiality and criticality of the activity cloud is being used to support to the overall activities of provider.
- Substitutability to replace the cloud provider in the event of an issue arising either through bringing the activity back in house or sourcing an alternative provider.
- The availability of alternative providers in the market.
- Benefits and risks associated with the cloud arrangement in terms of meeting customer commitments and regulatory requirements.
- Where the cloud infrastructure in question is using public or private cloud.
- The type of cloud arrangement, i.e. whether it is IaaS, PaaS or SaaS.

We feel it is very important for EIOPA to acknowledge that the wide range of types of cloud arrangements possible means that a single governance standard is not appropriate for them all.
In addition, Irish Life Group would have a concern that a challenge may arise where the current Guidelines overlap with other legislative and regulatory requirements, where the principle of proportionality is not explicitly called out. For example EIOPA Explanatory Text supporting its Guidelines on System of Governance notes that:

> *"in determining whether an outsourced function or activity is critical or important the undertaking has to take into account any definition or list of such functions or activities provided under national law or national administrative interpretation".*

Where these lists under national law or national administrative interpretation are not prefixed with the notion of proportionality they can never hope to capture any degree of proportionality when considered across different undertakings and the individual scale and complexity of each individual outsourcing arrangement. This can lead to binary, non-risk sensitive categorization of arrangements as critical or important and impose excessive governance expectations. E.g. in EIOPA Explanatory Text supporting its Guidelines on System of Governance, 'provision of data storage' is stated as an example of a critical or important function. This does not consider the nature, scale and complexity of the risks attaching to the specific data set being stored, storage location, etc.

Proportionality is of additional importance in the context of cloud services arrangements which are in constant development with undertakings needing to apply risk-sensitive proportionality to the

application of the Guidelines in the context of agile initiatives development. The industry is increasingly responding to the threat of disruption through innovation labs and agile proof of concept projects. Supervisors typically accept the value of such programmes but challenges can arise around regulatory expectations such as from the draft Guidelines on outsourcing to cloud service providers if the principle of proportionality is not applied. We would urge EIOPA to consider clarifying its expectations where jurisdictional supervisory bodies have not implemented 'regulatory sandbox' regimes in support of industry agile innovation labs.

From an Irish Life perspective, we take a tiered approach, with Tier1 being the most important and Tier 4 being the least important. There are two main drivers we consider when weighting for proportionality:

- The presence of personally identifiable information (PII)
- Risk-prioritised resiliency requirements

The above are broadly driven by the potential negative consequence should some adverse event occur.

As a Tier 1 example relating to personally identifiable information (PII), in the event that a cloud implementation involves storage of large volumes of PII, or special categories of personal data regarding customers pensions (health data), we are most concerned about the potential impact of a fine under the General Data Protection Regulations (GDPR). However, as an alternate Tier 3 example, we would be less concerned about an online training system where only an employee's name and email address might be captured.

It should be noted that per our risk operating model, in the above examples the same level of due diligence would be carried out by ISO & Privacy units within our business.

Further, we also engage with suppliers that we weight as Tier 4 contracts; these typically do not include PII and/or do not require a high level of resilience. With that in mind, the level of due diligence carried out is minimal, as is proportional to the risk.

When assessing third party arrangements which are not held with cloud service providers but which rely significantly on cloud infrastructure, then the principle of materiality and proportionality will be key. Otherwise, the regulatory cost of implementing the guidelines will far outweigh any benefit to the undertaking.

Guideline 1

Irish Life Group disagrees with the assumption that an arrangement with a cloud service provider should prima facie be deemed outsourcing. It is unclear why cloud service providers should be singled out for this specific assumption.

In common with other EBA definitions and MiFID II Guideline definitions of outsourcing hinge on an arrangement where the "service provider performs a process, a service or an activity that would otherwise be undertaken by the institution itself". In many instances cloud services are used to carry out activities that an insurance undertaking would never be doing itself. For example, an insurer would not typically be in the business of developing its own software and as a result may well often source software externally, with SaaS arrangements being one option. In addition, what constitutes "an activity that would otherwise be undertaken" by a typical insurance undertaking will change over time in accordance with new market norms and the evolution of business models. Thus the internal definition of what constitutes 'outsourcing' for an undertaking may be expected to change over time. This will create scope for confusion and potential for inappropriate levels of

applied governance over certain suppliers should the Guideline deem all cloud service providers to be prima facie cases of outsourcing.

It is a significant assumption to indicate that "as a rule, outsourcing should be assumed". Designation as 'outsourcing' has significant implications under Solvency II, not least because in EIOPA Explanatory Text supporting its Guidelines on System of Governance indicates that "in determining whether an outsourced function or activity is critical or important the undertaking has to take into account any definition or list of such functions or activities provided under national law or national administrative interpretation". Such definitions and lists may not always be pre-fixed with the notion of proportionality or a notion of proportionality that is consistent with that espoused by EIOPA's own guidelines. As an example, in EIOPA Explanatory Text supporting its Guidelines on System of Governance 'provision of data storage' is stated as an example of a critical or important function. Dependent on the interpretation of the specific activities that constitute data storage this could lead to cloud suppliers "as a rule" being deemed to be outsourcing, and by definition of their data support structures, also 'critical or important'. This could lead to disproportionate and inconsistent levels of governance across members states compared to the risk if proportionality in not applied in relation to such things as the type and volume of the data being stored.

Conversely, EIOPA Explanatory Text supporting its Guidelines on System of Governance also indicates that "purchase of standardised services" cannot be considered 'critical or important'. However, background to this consultation states "compared with more traditional forms of outsourcing offering dedicated solutions to clients, cloud outsourcing services are much more standardised, which allows the services to be provided to a larger number of different customers in a much more automated manner and on a larger scale".

Clarity is needed on apparently contradictory statements contained in related guidelines and the interplay between the Guideline and separate definitions or lists of outsourced functions or activities (and their criticality) provided elsewhere under national law or national administrative interpretation.

Guideline 5

Clarity should be provided on whether what is envisaged is one central register or if the location of the data within a series of registers/lists within an undertaking is sufficient i.e. audit dates and next scheduled audits are generally held within the control functions rather than the outsource register.

Guideline 7

Guideline 7 states:

"Prior to entering into any outsourcing arrangement with cloud service providers, the undertaking should assess if the cloud outsourcing has to be considered 'material'. The assessment should take into account whether the cloud outsourcing is related to critical or important operational functions as referred to in the Solvency II Directive and in the Delegated Regulation and whether the cloud outsourcing is materially affecting the risk profile of the undertaking. In performing such assessment, where relevant, an undertaking should take into account the possible extension and foreseen changes to the cloud services' scope."

Irish Life would challenge a requirement that the materiality of a cloud service arrangement be determined based on possible extension or extension of the scope of those services. Heightened materiality will impose heightened levels of governance. This should only be required when foreseen changes are 'probable' or being implemented and should then form part of the due diligence carried out at that time.

Furthermore it is stated that:

"Moreover, in order to determine the materiality of cloud outsourcing, undertakings should take into account, together with the outcome of the risk assessment, at least the following factors…

… the undertaking's aggregated exposure to the same cloud service provider and the potential cumulative impact of outsourcing arrangements in the same undertaking's business area"

Clarity is sought on whether the intent is for an undertaking to consider concentration risk where cloud service providers offer direct services, or whether the intent also for an undertaking to consider concentration risk at a sub-contractor level. Irish Life is of the view that concentration risk should be considered where a cloud service provider is a direct provider of services to the undertaking, however, it may not be possible or feasible to consider concentration risk where the cloud provider is providing services to a third party who in turn provides services to the undertaking.

Clarity is also sought on whether the intent is for an undertaking to consider concentration risk within just their own business or also more broadly across their industry area. Irish Life is of the view that concentration risk should be considered within a business, but that it may not be possible or feasible for an individual business to consider concentration risk relating to cloud providers more broadly across the industry. Market concentration risk should be monitored and examined by the national competent authority.

Guideline 8

"The undertaking should assess the potential impact of material cloud outsourcing both before and after the outsourcing particularly on their operational risk, strategic risk, concentration risk and reputational risk. The assessment should include, where appropriate, scenario analysis of possible but plausible, including high-severity, operational risk events.

Moreover, within their risk assessment in case of material cloud outsourcing, the undertaking should also take into account the expected benefits and costs of the proposed cloud outsourcing arrangement performing a cost-benefit analysis to be approved, as part of the overall approval, by the AMSB."

Additional clarity is sought around the provision set out above and how the principle of proportionality interplays with the assessment underlined.

Supplier risk assessments are often a designated activity / process within organisations. Cost versus benefit analysis typically takes place as part of Business Case development with outputs from the two parallel processes included in any request for Board approval. Strict interpretation of "within their risk assessment" could require amalgamation of parallel processes which is presumably not the intention.

In addition, we would question why a number of the provisions within this Guideline are being addressed to cloud services providers given they are not cloud specific requirements.

Guideline 11

"The outsourcing agreement should not limit the undertaking's information, access and audit rights as well as control options on cloud services in order to fulfil all its regulatory obligations. Additionally, it should be ensured that the undertaking receives the information it needs to adequately manage and monitor the risks associated with cloud outsourcing arrangements."

Irish Life would like clarification of the extent to which an undertaking's requirements for information, access and audit rights as well as control options on cloud services can be tailored to the risk profile of the service and provider in question.

Our view is that the extent to which information, access and audit rights as well as control options on cloud services are available need only be sufficient to adequately manage and monitor the risks associated with cloud outsourcing arrangements. As examples:

- The right to audit may not be necessary where the provider is an industry standard provider and makes an appropriate assurance report available to their customers;

- The ability to configure controls depends on the nature of the service and the provider. Many of the configuration settings are defined by the service provider for PAAS or SAAS solutions. An appropriate assurance report may provide comfort that these are appropriate.

"…. Undertakings may use….third party certifications and third-party or internal audit reports made available by the cloud service provider; pooled audits (i.e. performed jointly with other clients of the same cloud service provider), audit performed by third clients or by a third party appointed by them. .. only if they have the contractual right to request the expansion of the scope of the certifications or audit reports to other relevant systems and controls."

Irish Life would like clarification on the expectation of having a 'contractual right to request the expansion of the scope'. Generally the content of assurance reports or third party certification should be considered as part of due diligence process to ensure it provides appropriate coverage. In normal circumstances an undertaking can request a change to the scope of the assurance report or certification (as with any service). This can be done at the point of engaging with the vendor or if this is required due to a change in services or processes. However, the right to request is generally not enshrined within a contract in the Irish market.

Guideline 12

"For the purposes of the previous paragraph, an undertaking, prior to outsource to cloud service providers, on the basis of the results of the risk assessment performed in accordance with Guideline 8, should …….. monitor the level of fulfilment of the requirements relating to the efficiency of control mechanisms implemented by the cloud service provider and its significant sub-outsourcers that would mitigate the risks related to the provided services."

Irish Life would like clarification relating to the nature and extent of monitoring that would be expected to be carried out. A 'one size fits all' approach taken to all outsourcing would be difficult and time consuming to complete. Additional guidance relating to prioritisation based on risk would

be beneficial. It may be further worth clarifying if the engagement of service auditors or reliance on 3rd party certifications as highlighted in Guideline 11 would be sufficient to address the intent of this monitoring.

Guideline 13

"To comply with the requirements of Article 274(4)(k) and (l) of the Delegated Regulation, the cloud outsourcing agreement should specify, where relevant, whether or not sub-outsourcing of critical or important functions or activities of the undertaking, or significant parts thereof, are permitted or expressly excluded. The undertaking should agree to sub-outsource only if the sub-outsourcer will also fully comply with the obligations existing between the undertaking and the cloud service provider. These obligations include the audit and access rights and the security of data and systems as defined by the Solvency II Directive and the Delegated Regulation and further specified by these Guidelines."

It is the view of Irish Life that the scope of this guideline should be reduced to apply only to relevant contractual obligations and allow for reliance to be placed on third party contractual provisions.

Conclusion

The nature and scale of services that can now be accessed via cloud services providers is constantly increasing and will continue to do so for the foreseeable future. In addition, cloud service providers hold very technical experience on a number of areas including security benefits which are core to their business.

Irish Life Group welcomes the publication of the Guidelines by EIOPA but would stress as stated above the need to ensure proportionality and materiality when putting in place new Guidance.

Irish Life would like to note that its experience, albeit that the Irish Life Group is the largest financial services group in Ireland have found the negotiation of changes to standard contractual terms and conditions with cloud services providers exceptionally difficult. The expectation therefore that insurance undertakings of all sizes and scale will be able to negotiate changes to align with these Guidelines is questionable.

Irish Life would welcome the opportunity to meet with EIOPA to discuss any of the above.