

Gabriel Bernardino

Chairman

European Insurance and Occupational Pensions Authority (EIOPA)

Westhafen Tower, Westhafenpl. 1

60327 Frankfurt am Main

Germany

Pan-European Insurance Forum's recommendations for EIOPA's guidelines on outsourcing to the Cloud

16 November 2018

Dear Mr Bernardino,

dear Gabriel,

As part of their wider digital transformation strategies, many EU (re)insurers are expanding their use of the Cloud. We understand that this is also a topic for EIOPA given the EU Commission's FinTech Action plan and developments at national level. Earlier this year, the European Banking Authority (EBA) issued its recommendations on outsourcing to Cloud service providers. We understand that the guidelines will be used to inform EIOPA's own work. In light of these developments, the PEIF would like to share its views on regulatory issues associated with the use of the Cloud and the appropriateness of the EBA recommendations for our sector:

- **Materiality assessment and involvement of supervisors.** We agree that regulated firms have an overall responsibility to ensure that the relationship with the Cloud service provider is appropriately managed and controlled. This includes assessing which outsourcing activities should be considered as material and gaining timely regulatory approval (where required) from the competent authorities to ensure business agility. There should be no retroactive supervisory approval for activities already placed on the cloud in line with pre-existing local regulations. Not all uses of Cloud should be considered as material outsourcing for regulatory purposes. A risk-based approach should be adopted and only where the use of Cloud is material to core business processes or can otherwise have a material impact on the business operations should it be considered as material outsourcing. The PEIF is of the view that regulators should not prescribe how financial institutions should manage the outsourcing to the Cloud provider. For instance, the regulator should not impose on (re)insurers which Cloud service providers should be used. Furthermore, EIOPA guidelines should seek to harmonize existing local requirements, primarily in relation to a common view of materiality and not result in additional requirements or layers of approval.
- **Access and audit rights.** The EBA as well as some other regulators continue to recommend or request unrestricted audit rights (including on-site audits) in connection with outsourcing to the Cloud. While we agree with the general requirement of unrestricted audit rights in relation to outsourced functions and activities, in the case of the Cloud on-site audits should be restricted to exceptional

circumstances only. On-site audits are not necessary to achieve supervisory objectives and give limited insights into service performance; more relevant is the provider's compliance with laws and information security standards.

Furthermore, in particular in case of small and medium-size insurance companies, their audit departments often do not have the necessary skill set needed to conduct effective on-site audits of Cloud providers. The high number of audit teams conducting audits on-site, sometimes even in parallel, could severely impact the day-to-day operations of the Cloud provider and unintentionally lead to a less secure environment.

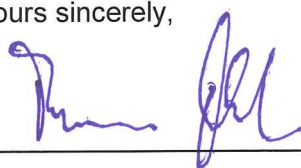
Supervisors, therefore, should rely on independent assurance by third parties or compliance with the relevant ISO standards. For example, regulators could ask for Service Organization Control (SOC) reports or recent reports of test execution and vertical certification in the cloud environment (i.e. 27017 or STAR certification). Such reports are widely used within the industry and contain valuable information required to assess and address the risks associated with an outsourced service. The adherence to the frameworks and standards are the cloud service providers' responsibility.

- **Contingency plans and data portability clauses.** We agree with the EBA that the outsourcing contract should include a termination and data portability clause that allows the activities to be transferred to another outsourcing service provider or to be reincorporated into the outsourcing institution if necessary. PEIF companies have frameworks in place in order to ensure operational resilience, regardless of whether the service is provided in house or outsourced to the Cloud. As servers become increasingly standardised, as is the case with the public Cloud, it is much easier to reinstall the servers in case of a cyber incident or an operational breakdown. Furthermore, Cloud service providers normally include business continuity features in their operations which ensures data is automatically backed up and accessible within its data centres. Therefore, less customised servers tend to be more operationally resilient.
- **Expectations in terms of data protection and information security.** Although not directly addressed by the EBA's recommendations, we have seen some regulatory misconceptions related to the safety and compliance of the public Cloud with the data protection requirements. From the PEIF's perspective, security in the public Cloud is highly sophisticated and often superior to what an individual entity could maintain. Moreover, cloud users know where data centres are located and from where maintenance/support work is performed. We would welcome efforts by EIOPA to facilitate knowledge sharing sessions with supervisors e.g. through its InsurTech taskforce meetings.
- **Regulatory coordination and a framework for mutual recognition.** One important point missing from the EBA's recommendation is the need for regulators globally to adopt a transparent and consistent approach for approving Cloud use which includes a framework for mutual recognition. Currently, companies normally have to notify or gain a regulatory approval for the use of the Cloud from each of its supervisors. We think that once regulatory approval is granted by the group supervisor, this supervisory approval should be recognised by other supervisors. Furthermore, more consistency in the regulatory approach on the use of the Cloud is needed across different jurisdictions to avoid conflicting requirements e.g. on data localisation.
- **Risks could be most effectively addressed by regulating the Cloud service providers directly.** The supply of cloud infrastructure is currently concentrated with a rather limited number of providers. While we understand the rationale for imposing regulatory requirements on the financial institutions

which outsource certain functions to the Cloud service providers, we think that the Cloud market dynamics make such supervisory practices not fully efficient and there could be other ways of addressing it, including through direct supervision. Minimum requirements for Cloud providers regarding business continuity, data protection and information security would build trust and avoid the need for multiple industry standards finally also making compliance for cloud providers easier and more transparent.

We thank you in advance for your consideration of these issues and would welcome the opportunity to discuss them in more detail with you or your colleagues. We believe that we can bring several constructive ideas to that would contribute positively to policy reflection in this area.

Yours sincerely,

A handwritten signature in blue ink, consisting of a stylized first name and a last name, positioned above a horizontal line.

Chairman of the Pan-European Insurance Forum

About the Pan-European Insurance Forum (PEIF)

PEIF is an informal forum for the CEOs of major European insurers (Aegon, Allianz, AVIVA, AXA, Generali, MAPFRE, Munich Re, RSA, Swiss Re, UNIQA, and Zurich) to exchange and present views on policy and regulatory issues amongst themselves and with others. PEIF companies represent around two-thirds of the STOXX® Europe Insurance.

EU Transparency Register: 03667978021-69