JUL. 21

INFORMATIVE NOTE

DISPUTE RESOLUTION

Outsourcing to cloud computing service providers

Circular 3/2021

The European Insurance and Occupational Pensions Authority ("EIOPA") is entrusted with[1] issuing guidelines and recommendations to Member States' supervisory authorities on how insurance and reinsurance undertakings should apply the Solvency II Directive[2] in order to (i) establish consistent, efficient and effective supervisory practices and (ii) ensure the common, uniform and consistent application of Union law.

In this context, the EIOPA guidelines on outsourcing to cloud computing service providers[3] ("Guidelines") were published on 6 February 2020. On 1 January 2021, these guidelines began to apply to all outsourcing agreements made or amended on or after that date and they are intended to be implemented by 31 December 2022.

"The EIOPA guidelines on outsourcing to cloud computing service providers were published."

In turn, on 11 May 2021, the Portuguese Insurance and Pension Funds Supervisory Authority[4] ("ASF") issued Circular 3/2021, in which it announced its intention to launch a public consultation on the draft Regulatory Standard that will incorporate these Guidelines. It will also address diagnostic questionnaires to the Portuguese insurance market to identify the experience of insurance companies regarding the digital innovations in question.

Regardless of the advances in terms of regulation by the ASF and of the date the Regulatory Standard is published, a brief analysis of the Guidelines already published by the EIOPA is urgently required. Insurance companies have been concerned about the adaptations the Portuguese regulator will require in terms of outsourcing processes.

Margarida Ferraz de Oliveira
Paula Bento Neto
Dispute Resolution team

1 By virtue of Article 16 of Regulation (EU) No 1094/2010 of the European Parliament and of the Council of 24 November 2010.
2 Directive 2009/138/EC of the European Parliament and of the Council of 25 November 2009.
3 EIOPA-BoS-20-002, available here.
4 *Autoridade de Supervisão de Seguros e Fundos de Pensões.*

"Insurance undertakings will have to review current outsourcing arrangements relating to critical or important operational functions or activities and amend them in accordance with the Guidelines."

1. Scope of application

The Guidelines apply to "*services provided using cloud computing, that is, a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction*"[5].

However, the Guidelines only apply to outsourcing for the purposes of the Solvency II Directive and this is defined as: "*an arrangement of any form between an insurance or reinsurance undertaking and a service provider, whether a supervised entity or not, by which that service provider performs a process, a service or an activity, whether directly or by sub-outsourcing, which would otherwise be performed by the insurance or reinsurance undertaking itself*"[6].

Insurance undertakings will have to review current outsourcing arrangements relating to critical or important operational functions or activities and amend them in accordance with the Guidelines. If this review is not completed by 31 December 2022, insurance undertakings will be required to inform the ASF of this and tell it about the steps they have planned to complete the review and any exit strategy for those arrangements.

2. General principles of governance for cloud outsourcing[7]

First, the insurance undertaking's administrative, management or supervisory body should ensure that any decision to outsource these services is based on a thorough risk assessment, including all the weaknesses that may be inherent to the outsourcing[8].

Where critical operational functions or activities are outsourced, the insurance undertaking must, where relevant, address the changes that the outsourcing entails in its risk profile and in its internal risk and solvency assessment.

Furthermore, when using cloud computing services, insurance undertakings should take into account their existing strategies and be consistent with them. These include their information and communication technology ("ICT"), information security and operational risk management strategies, as well as their internal policies and processes – and these should be updated as necessary.

5 See definition of "Cloud services", paragraph 9 of the Guidelines.
6 See article 13(28) of the Solvency II Directive.
7 See Guideline 2 of the Guidelines.
8 Notwithstanding Article 274(3) of Commission Delegated Regulation (EU) 2015/35 of 10 October 2014 ("Delegated Regulation").

3. Updating of the outsourcing policy

With regard to updating the outsourcing policy, the EIOPA wanted to ensure that, when outsourcing to cloud computing service providers, the insurance company has its outsourcing policy (and other relevant internal policies) updated in accordance with the specific characteristics of the cloud services contracted. The following matters, in particular, must be updated:

"The EIOPA wanted to ensure that, when outsourcing to cloud computing service providers, the insurance company has its outsourcing policy updated."

i) roles and responsibilities of the insurance company bodies and individuals involved in the outsourcing;

ii) processes and reporting procedures required for the approval, execution, management and renewal of outsourcing arrangements;

iii) supervision of cloud services proportionate to the nature, scale and complexity of the risks associated with the services provided;

iv) contractual requirements, as described in Guideline 10, for the outsourcing of services relating to critical or important operational functions;

v) requirements for documentation and written notification to the ASF of the outsourcing of services relating to critical or important operational functions; and finally,

vi) for each outsourcing arrangement for critical or important operational functions or activities, the definition of a documented "exit strategy".

4. Written notification to the ASF[9]

The written notification requirements set out in Article 49(3) of the Solvency II Directive and specified in the EIOPA Governance Guidelines apply to all outsourcing of critical or important operational functions and activities to cloud computing service providers. Where an outsourced operational function or activity that was previously classified as non-core or non-important becomes core or important, the undertaking must notify the ASF of the change.

For this purpose, the EIOPA defines the minimum content of the written notification to the national regulator.

PL
MJ

9 See Guideline 4 of the Guidelines.

5. Documentation requirements

The insurance undertaking should keep a record of information on the outsourcing agreements for cloud computing services that are in place, and keep records of terminated agreements for an appropriate period of time and in accordance with national law.

For the outsourcing of services relating to core operational functions, the EIOPA defines what the minimum content of those records should be.

6. Assessment of critical operational functions and activities

Before entering into any outsourcing arrangement, the undertaking must assess whether the outsourcing arrangement concerns an operational function or activity that is critical or important or may become critical or important in the future. Furthermore, the critical nature or significance should also be reassessed if there is any change in the nature, scale or complexity of the risks inherent to the arrangement.

When this assessment is made, the undertaking should take into account, in conjunction with the outcome of the risk assessment:

"The undertaking should take into account, in conjunction with the outcome of the risk assessment, the size and complexity of any area of activity affected by the outsourcing arrangement."

i) the potential impact of any significant disruption to the outsourced operational function or activity or the inability of the cloud service provider to provide the services at agreed service levels;

ii) the potential impact of the cloud computing outsourcing arrangement on the undertaking's ability to manage risk, comply with the law and perform audits;

iii) the undertaking's overall exposure to the same cloud service provider and the potential impact of cumulative outsourcing arrangements in the same area of activity;

iv) the size and complexity of any area of activity affected by the outsourcing arrangement;

v) the ability to transfer the proposed outsourcing arrangement to another cloud computing service provider, if necessary; and

vi) the protection of personal and non-personal data and the potential impact on the undertaking, policyholders or other relevant data subjects of a breach of confidentiality or the inability to ensure data availability and integrity[10].

10 As provided for in Regulation (EU) No 2016/679 of the European Parliament and of the Council of 27 April 2016.

7. Risk assessment

Before entering into any agreement with a cloud computing service provider, the insurance undertaking should identify and assess all relevant risks, in particular operational and reputation risks.

Where this is a critical or important operational function or activity, undertakings should take into account:

i) the expected benefits and costs of the outsourcing arrangement, including consideration of any significant risks that could be mitigated; and

ii) the legal, ICT, compliance and reputation risks and the supervisory constraints relating to the service.

If, after the conclusion of the agreement, the insurance undertaking becomes aware of serious deficiencies or significant changes in the services provided or the provider's situation, the risk assessment should be reviewed or done again.

8. Due Diligence regarding service providers

The insurance undertaking should carry out appropriate due diligence on the prospective cloud computing service provider and ensure that it is suitable in the light of its outsourcing policy.

Where the undertaking enters into a second agreement with a cloud service provider that has already been assessed, it should determine, based on risks, whether a second assessment is necessary to fulfil the duty of due diligence.

If a serious deficiency or significant change in the service provided or concerning the provider is discovered, the insurance undertaking should review or even repeat the due diligence exercise.

When outsourcing critical or important operational functions, the due diligence should include an assessment of the suitability of the cloud service provider, for example as regards its skills, infrastructure, financial situation, business and legal status. These characteristics can be demonstrated with international certifications, recognised third-party audit reports or internal audit reports.

"If a serious deficiency or significant change in the service provided or concerning the provider is discovered, the insurance undertaking should review or even repeat the due diligence exercise."

PL
MJ

9. Final Notes

Regarding specific outsourcing agreements, the Guidelines also provide for (i) contractual requirements, such as the conclusion of a written agreement, (ii) access and audit rights that the provider must grant to the insurance undertaking, (iii) guarantees as to the security of data and systems, and (iv) termination rights and exit strategies.

"Regarding specific outsourcing agreements, the Guidelines also provide for access and audit rights that the provider must grant to the insurance undertaking."

It is therefore crucial for the national competent authorities in each Member State to confirm to the EIOPA whether and how they intend to adopt the Guidelines in their legal system and incorporate them appropriately into the regulatory or supervisory framework.

In summarising the measures introduced by the Guidelines, it is clear that, when applying, enforcing and monitoring the Guidelines, insurance undertakings and competent authorities should take into account the principle of proportionality[11] and the critical or important nature of the outsourced service. ■

11 See Article 29(3) of the Solvency II Directive.