boulevard de Berlaimont 14 – BE-1000 Brussels
Phone: + 32 2 221 44 74
Company number: 0203.201.340
RPM (Trade Register) Brussels
www.nbb.be

BanqueNationaleBank DE BELGIQUE VAN BELGIË
Eurosystem

Circular

Brussels, 5 May 2020

Reference: NBB_2020_018

Contact person:
Nicolas Strypstein
Phone: + 32 2 221 44 74
nicolas.strypstein@nbb.be

Recommendations of the Bank on outsourcing to cloud service providers

Scope

This Circular applies to:

- *insurance and reinsurance companies governed by Belgian law that are subject to the Law of 13 March 2016 on the legal status and supervision of insurance or reinsurance companies (with the exception of the insurance companies referred to in Articles 275, 276 or 294 of the aforementioned Law of 13 March 2016);*
- *authorised branches in Belgium of insurance companies of which the registered office is established in a third country (a country that is not a party to the European Economic Area (EEA) Agreement); and*
- *entities responsible*[1] *for an insurance or reinsurance group under Belgian law within the meaning of Articles 339, 2° and 343 of the Law of 13 March 2016 or for a financial conglomerate under Belgian law within the meaning of Articles 340, 1° and 343 of the Law of 13 March 2016.*

Summary/Objectives

This Circular specifies the recommendations of the National Bank of Belgium (the Bank) on outsourcing to cloud service providers. It implements the guidelines of the European Insurance and Occupational Pensions Authority (EIOPA) on the subject and applies from 1 January 2021.

This Circular also stipulates the Bank's approach to reporting. In this regard, it should be read in conjunction with Chapter 7 of the Overarching Circular on System of Governance NBB_2016_31, which specifies the Bank's general recommendations on outsourcing (which were recently revised through Communication NBB_2020_017).

[1] And more precisely insurance or reinsurance companies under Belgian law which are participating undertakings in at least one insurance or reinsurance company from the European Economic Area or from a third country, insurance or reinsurance companies under Belgian law of which the parent company is a mixed insurance holding company or a mixed financial holding company from the European Economic Area or from a third country, and insurance holding companies or mixed financial holding companies under Belgian law that are parent companies of an insurance or reinsurance company under Belgian law, insofar as these are subject to the provisions of the Law of 13 March 2016.

Dear Sir,
Dear Madam,

In accordance with Article 92 of the Law of 13 March 2016 on the legal status and supervision of insurance or reinsurance companies (hereinafter the "Insurance Supervision Law"), each insurance or reinsurance company should take the necessary measures to ensure that the use of outsourcing does not lead to any of the following: (i) materially impairing the quality of the company's governance system, (ii) unduly increasing the operational risk, (iii) impairing the ability of the National Bank of Belgium (the "Bank") to monitor the company's compliance with its legal and regulatory obligations and (iv) undermining continuous and satisfactory service to policyholders, insured and beneficiaries of insurance policies or the persons concerned by the execution of reinsurance policies.

The general rules on outsourcing are set out in Article 274 of Delegated Regulation 2015/35 of 10 October 2014 supplementing the Solvency II Directive (hereinafter "Delegated Regulation 2015/35") and in Chapter 7 of the Overarching Circular on System of Governance NBB_2016_31 (this Chapter was recently updated through Communication NBB_2020_017).

In this Circular, the Bank provides special additional recommendations for the specific case of outsourcing to cloud service providers. These recommendations transpose the Guidelines on outsourcing to cloud service providers, as published by EIOPA on 6 February 2020, into Belgian regulations.

1. Recommendations of the Bank

Definitions

For the purposes of this Circular, the following definitions apply:

- "company": an insurance or reinsurance company included in the scope defined above;
- "service provider": a third-party entity that performs a process, service or activity, or parts thereof, under an outsourcing arrangement;
- "cloud service provider": a service provider, as defined above, responsible for delivering cloud services under an outsourcing arrangement;
- "cloud services": 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 effort or service provider interaction;
- "public cloud": cloud infrastructure available for open use by the general public;
- "private cloud": cloud infrastructure available for the exclusive use by a single company;
- "community cloud": cloud infrastructure available for the exclusive use by a specific community of companies, e.g. several companies of a single group;
- "hybrid cloud": cloud infrastructure that is composed of two or more distinct cloud infrastructures.

Recommendation 1 – Cloud services and outsourcing

The company should establish whether an arrangement with a cloud service provider falls under the definition of outsourcing pursuant to the Insurance Supervision Law.

As part of this assessment, consideration should be given to:
a. whether the operational function or activity (or a part thereof) outsourced is performed on a recurrent or an ongoing basis; and
b. whether this operational function or activity (or a part thereof) would normally fall within the scope of operational functions or activities that would or could be performed by the company in the course of its

regular insurance or reinsurance activities, even if the company has not performed this operational function or activity in the past.

Where an arrangement with a service provider covers multiple operational functions or activities, the company should take all aspects of the arrangement into account in its assessment.

In cases where the company outsources operational functions or activities to service providers which are not cloud service providers but rely significantly on cloud infrastructures to deliver their services (for example, where the cloud service provider is part of a sub-outsourcing chain), the arrangement for such outsourcing falls within the scope of these Recommendations.

Recommendation 2 – General principles of governance for cloud outsourcing

Without prejudice to Article 274(3) of Delegated Regulation 2015/35, the company's board of directors and management committee should ensure that any decision to outsource critical or important operational functions or activities to cloud service providers is based on a thorough risk assessment, including all relevant risks implied by the arrangement such as information and communication technology ("ICT"), business continuity, legal and compliance (including confidentiality), concentration, other operational risks, and risks associated to the data migration and/or the implementation phase, where applicable.

In case of outsourcing to cloud service providers of critical or important operational functions or activities, the company, where appropriate, should reflect the changes in its risk profile due to its cloud outsourcing arrangements in its own risk and solvency assessment ("ORSA").

The use of cloud services should be consistent with the company's strategies (for example, ICT strategy, information security strategy, operational risk management strategy) and internal policies and processes, which should be updated, if needed.

Recommendation 3 – Update of the written outsourcing policy

In case of outsourcing to cloud service providers, the company should update the **written outsourcing** policy (for example, by reviewing it, adding a separate appendix or developing new dedicated policies) and the other relevant internal policies (for example, information security), taking into account cloud outsourcing specificities at least in the following areas:

a. the roles and responsibilities of the company's functions involved, in particular the board of directors and the management committee, and the functions responsible for ICT, information security, compliance, risk management and internal audit;
b. the processes and reporting procedures required for the approval, implementation, monitoring, management and renewal, where applicable, of cloud outsourcing arrangements related to critical or important operational functions or activities;
c. the oversight of the cloud services proportionate to the nature, scale and complexity of risks inherent in the services provided, including (i) risk assessment of cloud outsourcing arrangements and due diligence on cloud service providers, including the frequency of the risk assessment, (ii) monitoring and management controls (for example, verification of the service level agreement), (iii) security standards and controls;
d. with regard to cloud outsourcing of critical or important operational functions or activities, a reference should be made to the contractual requirements as described in Recommendation 8;
e. documentation requirements and written notification to the supervisory authority regarding cloud outsourcing of critical or important operational functions or activities;
f. with regard to each cloud outsourcing arrangement that covers critical or important operational functions or activities, a requirement for a documented and, where appropriate, sufficiently tested 'exit strategy' that is proportionate to the nature, scale and complexity of the risks inherent in services provided. The exit strategy may involve a range of termination processes, including but not necessarily limited to, discontinuing, reintegrating or transferring the services included in the cloud outsourcing arrangement.

Recommendation 4 – Pre-outsourcing analysis

Before entering into any arrangement with cloud service providers, the company should:

a. assess if the cloud outsourcing arrangement concerns a critical or important operational function or activity in accordance with Recommendation 5;
b. identify and assess all relevant risks of the cloud outsourcing arrangement in accordance with Recommendation 6;
c. undertake appropriate due diligence on the prospective cloud service provider in accordance with Recommendation 7;
d. identify and assess conflicts of interest that the outsourcing may cause in line with the requirements set out in Article 274(3)(b) of Delegated Regulation 2015/35.

Recommendation 5 – Assessment of the criticality or importance of cloud outsourcing

Prior to entering into any outsourcing arrangement with cloud service providers, the company should assess if the cloud outsourcing arrangement relates to an operational function or activity that is critical or important. In performing such an assessment, where relevant, the company should consider whether the arrangement has the potential to become critical or important in the future. The company should also reassess the criticality or importance of the operational function or activity previously outsourced to cloud service providers, if the nature, scale and complexity of the risks inherent in the agreement materially change.

In the assessment, the company should take into account, together with the outcome of the risk assessment, at least, the following factors:

a. the potential impact of any material disruption to the outsourced operational function or activity or failure of the cloud service provider to provide the services at the agreed service levels on the company's: i. continuous compliance with its regulatory obligations; ii. short and long-term financial and solvency resilience and viability; iii. business continuity and operational resilience; iv. operational risk, including conduct, ICT and legal risks; v. reputational risks;
b. the potential impact of the cloud outsourcing arrangement on the ability of the company to: i. identify, monitor and manage all relevant risks; ii. comply with all legal and regulatory requirements; iii. conduct appropriate audits regarding the operational function or activity outsourced;
c. the company's (and/or group's, where applicable) aggregated exposure to the same cloud service provider and the potential cumulative impact of outsourcing arrangements in the same business area;
d. the size and complexity of any of the company's business areas affected by the cloud outsourcing arrangement;
e. the ability, if necessary or desirable, to transfer the proposed cloud outsourcing arrangement to another cloud service provider or reintegrate the services ("substitutability");
f. the protection of personal and non-personal data and the potential impact on the company, policyholders or other relevant subjects of a confidentiality breach or failure to ensure data availability and integrity based on inter alia Regulation (EU) 2016/679. The company should particularly take into consideration data that is business secret and/or sensitive (for example, policyholders' health data).

Recommendation 6 – Risk assessment of cloud outsourcing

In general, the company should adopt an approach proportionate to the nature, scale and complexity of the risks inherent in the services outsourced to cloud service providers. This includes assessing the potential impact of any cloud outsourcing, in particular on their operational and reputational risks.

In case of outsourcing of critical or important operational functions or activities to cloud service providers, the company should:

a. take into account the expected benefits and costs of the proposed cloud outsourcing arrangement, including weighing any significant risks which may be reduced or better managed against any significant risks which may arise as a result of the proposed cloud outsourcing arrangement;

b. assess, where applicable and appropriate, the risks, including legal, ICT, compliance and reputational risks, and the oversight limitations arising from:

   i. the selected cloud service and the proposed deployment models (i.e. public/private/hybrid/community);
   ii. the migration and/or the implementation;
   iii. the activities and related data and systems which are under consideration to be outsourced (or have been outsourced) and their sensitivity and required security measures;
   iv. the political stability and the security situation of the countries (within or outside the EU) where the outsourced services are or may be provided and where the data are or are likely to be stored. The assessment should consider: 1. the laws in force, including laws on data protection; 2. the law enforcement provisions in place; 3. the insolvency law provisions that would apply in the event of a service provider's failure and any constrains that would arise with regard to the urgent recovery of the company's data;
   v. sub-outsourcing, including the additional risks that may arise if the subcontractor is located in a third country or a different country from the cloud service provider and the risk that long and complex chains of sub-outsourcing reduce the ability of the company to oversee its critical or important operational functions or activities and the ability of supervisory authorities to effectively supervise them;
   vi. the company's overall concentration risk to the same cloud service provider, including outsourcing to a cloud service provider that is not easily substitutable or multiple outsourcing arrangements with the same cloud service provider.

When assessing the concentration risk, the company (and/or the group, where applicable) should take into account all its cloud outsourcing arrangements with that cloud provider.

The risk assessment should be performed before entering into a cloud outsourcing. If the company becomes aware of significant deficiencies and/or significant changes to the services provided or to the situation of the cloud service provider, the risk assessment should be promptly reviewed or re-performed. In case of renewal of a cloud outsourcing arrangement concerning its content and scope (for example, enlargement of the scope or inclusion in the scope of critical or important operational functions previously not included), the risk assessment should be re-performed.

Recommendation 7 – Due diligence on the cloud service provider

The company should ensure in its selection and assessment process that the cloud service provider is suitable for providing the relevant services according to the criteria defined by its written outsourcing policy (due diligence process).

The due diligence on the cloud service provider should be performed prior to outsourcing any operational function or activity. In case the company enters into a second agreement with a cloud service provider that has already been assessed, the company should determine, on a risk-based approach, whether a second due diligence is needed. If the company becomes aware of significant deficiencies and/or significant changes to the services provided or to the situation of the cloud service provider, the due diligence should be promptly reviewed or re-performed.

In case of cloud outsourcing of critical or important operational functions, the due diligence should include an evaluation of the suitability of the cloud service provider (for example, skills, infrastructure, economic situation, corporate and regulatory status). Where appropriate, in order to support the due diligence

performed, the company can use evidence, certifications based on international standards, audit reports of recognised third parties or internal audit reports.

Recommendation 8 – Contractual requirements

The respective rights and obligations of the company and of the cloud service provider should be clearly allocated and set out in a written agreement.

Without prejudice to the requirements defined in Article 274 of Delegated Regulation 2015/35, in case of outsourcing of critical or important operational functions or activities to a cloud service provider, the written agreement between the company and the cloud service provider should set out:

a. a clear description of the outsourced function to be provided (cloud services, including the type of support services);
b. the start date and end date, where applicable, of the agreement and the notice periods for the cloud service provider and for the company;
c. the court jurisdiction and the governing law of the agreement;
d. the parties' financial obligations;
e. whether the sub-outsourcing of a critical or important operational function or activity (or material parts thereof) is permitted, and, if so, the conditions to which the significant sub-outsourcing is subject to (see Recommendation 11);
f. the location(s) (i.e. regions or countries) where relevant data will be stored and processed (location of data centres), and the conditions to be met, including a requirement to notify the company if the service provider proposes to change the location(s);
g. provisions regarding the accessibility, availability, integrity, confidentiality, privacy and safety of relevant data, taking into account the specifications of Recommendation 10;
h. the right for the company to monitor the cloud service provider's performance on a regular basis;
i. the agreed service levels which should include precise quantitative and qualitative performance targets in order to allow for timely monitoring so that appropriate corrective actions can be taken without undue delay if agreed service levels are not met;
j. the reporting obligations of the cloud service provider to the company, including, as appropriate, the obligations to submit reports relevant for the company's security function and key functions, such as reports of the internal audit function of the cloud service provider;
k. whether the cloud service provider should take mandatory insurance against certain risks and, if applicable, the level of insurance cover requested;
l. the requirements to implement and test business contingency plans;
m. the requirement for the cloud service provider to grant the company, its supervisory authorities and any other person appointed by the company or the supervisory authorities, the following: i. full access to all relevant business premises (head offices and operation centres), including the full range of relevant devices, systems, networks, information and data used for providing the outsourced function, including related financial information, personnel and the cloud service provider's external auditors ("access rights"); ii. unrestricted rights of inspection and auditing related to the cloud outsourcing arrangement ("audit rights"), to enable them to monitor the outsourcing arrangement and to ensure compliance with all applicable regulatory and contractual requirements;
n. provisions to ensure that the data owned by the company can be promptly recovered by the company in case of insolvency, resolution or discontinuation of business operations of the cloud service provider.

Recommendation 9 – Access and audit rights

The cloud outsourcing agreement should not limit the company's effective exercise of access and audit rights as well as control options on cloud services in order to fulfil its regulatory obligations.

The company should exercise its access and audit rights and determine the audit frequency and the areas and services to be audited on a risk-based approach.

In determining the frequency and the scope of its exercise of access or audit rights, the company should consider whether the cloud outsourcing is related to a critical or important operational function or activity, and determine the nature and extent of the risk and the impact on the company from the cloud outsourcing arrangements.

If the exercise of its access or audit rights, or the use of certain audit techniques creates a risk for the environment of the cloud service provider and/or another customer of the cloud service provider (for example, the impact on service levels, availability of data, confidentiality aspects), the company and the cloud service provider should agree on alternative ways to provide a similar level of assurance and service to the company (for example, the inclusion of specific controls to be tested in a specific report/certification produced by the cloud service provider).

Without prejudice to their final responsibility regarding the activities performed by their cloud service providers, in order to use audit resources more efficiently and decrease the organisational burden on the cloud service provider and its customers, companies may use:

a. third-party certifications and third-party or internal audit reports made available by the cloud service provider;
b. pooled audits (i.e. performed jointly with other customers of the same cloud service provider), or pooled audits performed by a third party appointed by them.

In case of cloud outsourcing of critical or important operational functions or activities, companies should make use of third-party certifications and third-party or internal audit reports only if they:

a. ensure that the scope of the certification or the audit report covers the systems (for example, processes, applications, infrastructure, data centres, etc.) and the controls identified by the company and assess the compliance with relevant regulatory requirements;
b. thoroughly assess the content of new certifications or audit reports on a regular basis and verify that the certifications or reports are not obsolete;
c. ensure that key systems and controls are covered in future versions of the certification or audit report;
d. are reasonably certain about the aptitude of the certifying or auditing party (for example, with regard to rotation of the certifying or auditing company, qualifications, expertise, re-performance/verification of the evidence in the underlying audit file);
e. are reasonably certain that certifications are issued and that the audits are performed according to appropriate standards and include a test of the operational effectiveness of the key controls in place;
f. have the contractual right to request the expansion of the scope of the certifications or audit reports to other relevant systems and controls; the number and frequency of such requests for scope modification should be reasonable and legitimate from a risk management perspective;
g. retain the contractual right to perform individual on-site audits at their discretion with regard to the cloud outsourcing of critical or important operational functions or activities; such right should be exercised in case of specific needs that cannot be met through other types of interactions with the cloud service provider.

For outsourcing to cloud service providers of critical or important operational functions, the company should assess whether third-party certifications and reports as referred to in paragraph 5, under a., of this Recommendation are adequate and sufficient to comply with its regulatory obligations and, on a risk-based approach, should not rely solely on these reports and certificates over time.

Before a planned on-site visit, the party exercising its right of access (company, auditor or third party acting on behalf of the company or companies) should provide prior notice in a reasonable time period, unless an early prior notification has not been possible due to an emergency or crisis situation. Such notice should include the location and purpose of the visit and the personnel that will participate in the visit.

Considering that cloud solutions have a high level of technical complexity, the company should verify that the staff performing the audit – being its internal auditors or the pool of auditors acting on its behalf, or the

cloud service provider's appointed auditors – or, as appropriate, the staff reviewing the third-party certification or service provider's audit reports have acquired the appropriate skills and knowledge to perform the relevant audits and/or assessments.

Recommendation 10 – Security of data and systems

The company should ensure that cloud service providers comply with European and national regulations as well as appropriate ICT security standards.

In case of outsourcing of critical or important operational functions or activities to cloud service providers, the company should additionally define specific information security requirements in the outsourcing agreement and monitor compliance with these requirements on a regular basis.

For the purposes of the previous paragraph, in case of outsourcing of critical or important operational functions or activities to cloud service providers, the company, applying a risk-based approach, and taking into account its responsibilities and the ones of the cloud service provider, should:

a. agree on clear roles and responsibilities between the cloud service provider and the company in relation to the operational functions or activities affected by the cloud outsourcing, which should be clearly split;
b. define and decide on an appropriate level of protection of confidential data, continuity of activities outsourced, integrity and traceability of data and systems in the context of the intended cloud outsourcing;
c. consider specific measures, where necessary, for data in transit, data in memory and data at rest, for example, the use of encryption technologies in combination with an appropriate keys management;
d. consider the mechanisms of integration of the cloud services with the systems of the company, for example, the Application Programming Interfaces and a sound user and access management process;
e. contractually ensure that network traffic availability and expected capacity meet strong continuity requirements, where applicable and feasible;
f. define and decide on proper continuity requirements ensuring adequate levels at each level of the technological chain, where applicable;
g. have a sound and well-documented incident management process including the respective responsibilities, for example, by the definition of a cooperation model in case of actual or suspected incidents;
h. adopt a risk-based approach to data storage and data processing location(s) (i.e. country or region) and information security considerations;
i. monitor the fulfilment of the requirements relating to the effectiveness and efficiency of control mechanisms implemented by the cloud service provider that would mitigate the risks related to the provided services;
j. ensure that a copy of the data is stored in one or more locations outside the cloud service provider's head office that are secure and at sufficient distance from the head office to not be exposed to the same risks and, with regard to critical data, examine the feasibility of having a copy independently of the cloud service provider to be able to resume activities in the event of the service provider's permanent failure;
k. ensure that the access of administrators of the cloud services is protected by strong authentication solutions;
l. contractually ensure that administrators of the cloud service provider do not have permanent access to its systems and data, in accordance with the principle of least privilege;
m. examine whether appropriate solutions can be found to prevent any unwanted exposure of the data traffic between the company and the cloud service.

Recommendation 11 – Sub-outsourcing

If sub-outsourcing of critical or important operational functions (or a part thereof) is permitted, the cloud outsourcing agreement between the company and the cloud service provider should:

a. specify any types of activities that are excluded from potential sub-outsourcing;
b. indicate the conditions to be complied with in case of sub-outsourcing (for example, that the sub-contractor will also fully comply with the relevant obligations of the cloud service provider). These obligations include the audit and access rights and the security of data and systems;
c. indicate that the cloud service provider retains full accountability and oversight for the services sub-outsourced;
d. include an obligation for the cloud service provider to inform the company of any planned significant changes to the sub-contractors or the sub-outsourced services that might affect the ability of the service provider to meet its obligations under the cloud outsourcing agreement. The notification period for those changes should allow the company, at least, to carry out a risk assessment of the effects of the proposed changes before the actual change in the subcontractors or the sub-outsourced services comes into effect;
e. ensure, in cases where a cloud service provider plans changes to a subcontractor or sub-outsourced services that would have an adverse effect on the risk assessment of the agreed services, that the company has the right to object to such changes and/or the right to terminate and exit the contract.

Recommendation 12 – Monitoring and oversight of cloud outsourcing agreements

The company should monitor, on a regular basis, the performance of activities, the security measures and the adherence to the agreed service level by its cloud service providers on a risk-based approach. The main focus should be on the outsourcing of critical and important operational functions.

In order to do so, the company should set up monitoring and oversight mechanisms, which should take into account, where feasible and appropriate, the presence of sub-outsourcing of critical or important operational functions or a part thereof.

The management committee should be periodically updated on the risks identified in the cloud outsourcing of critical or important operational functions or activities.

In order to ensure the adequate monitoring and oversight of their cloud outsourcing agreements, companies should employ enough resources with adequate skills and knowledge to monitor the services outsourced to the cloud. The company's personnel in charge of these activities should have both ICT and business knowledge as deemed necessary.

Recommendation 13 – Termination rights and exit strategies

In case of cloud outsourcing of critical or important operational functions or activities, as part of the cloud outsourcing agreement the company should have a clearly defined exit strategy clause ensuring that it is able to terminate the agreement, where necessary. The termination should be made possible without detriment to the continuity and quality of its services to the insured. To achieve this, the company should:

a. develop exit plans that are comprehensive, service based, documented and sufficiently tested (for example, by carrying out an analysis of the potential costs, impacts, resources and timing implications of the various potential exit options);
b. identify alternative solutions and develop appropriate and feasible transition plans to enable the company to remove and transfer existing activities and data from the cloud service provider to alternative service providers or back to the company. These solutions should be defined with regard to the challenges that may arise because of the location of data, taking the necessary measures to ensure business continuity during the transition phase;
c. ensure that the cloud service provider adequately supports the company when transferring the outsourced data, systems or applications to another service provider or directly to the company;
d. agree with the cloud service provider that once retransferred to the company, its data will be completely and securely deleted by the cloud service provider in all regions.

When developing exit strategies, the company should consider the following:

a. define objectives of the exit strategy;
b. define the trigger events (for example, key risk indicators reporting an unacceptable level of service) that could activate the exit strategy;
c. perform a business impact analysis commensurate to the activities outsourced to identify what human and other resources would be required to implement the exit plan and how much time it would take;
d. assign roles and responsibilities to manage exit plans and transition activities;
e. define success criteria of the transition.

Recommendation 14 – Cloud outsourcing to a third country

Without prejudice to the provisions of Section 7.4.3. of the overarching circular on governance, outsourcing to a cloud service provider whose data are located outside the European Economic Area (in non-EEA or third countries) is permitted provided that the company can expressly guarantee that itself, its accredited statutory auditor and the Bank are able to exercise and enforce their access and audit rights in accordance with Article 307 of the Insurance Supervision Law. This implies that the company, its accredited statutory auditor and the Bank should have access to the data located outside the EEA at all times.

In addition to this general rule, cloud outsourcing to a service provider whose data are located in a third country, where this outsourcing is considered critical or important, is only permitted if the following conditions are met:

a. there is a cooperation agreement between the Bank and the prudential supervisory authority of the third country where the data are located or, if the cloud service provider is part of a group subject to supervision at group level in accordance with Directive 2009/138/EC (Article 343 of the Insurance Supervision Law), there is a coordination arrangement in relation to a supervisory college to which the Bank and the prudential supervisory authority of the third country are parties; and

b. the cooperation agreement or coordination arrangement referred to in point a. ensures that the Bank is at least able to, on the one hand, obtain the information necessary to carry out its tasks upon request and, on the other, obtain appropriate access to any data, documents, premises or personnel in the third country that are relevant for the performance of its supervisory powers (Article 307 of the Insurance Supervision Law).

However, these two conditions do not have to be met if the cloud service provider whose data are located in a third country makes these data available and auditable from a branch or subsidiary situated in the EEA.

Recommendation 15 – Retention of insurance documents

Specific rules apply if the cloud outsourcing relates to the retention of original copies of (i) insurance or reinsurance agreements (policies and riders), (ii) letters sent to policyholders and (iii) prudential reports required pursuant to the Insurance Supervision Law and to the Law of 4 April 2014 on insurance.

Article 76 of the Insurance Supervision Law provides that these documents should be kept at the company's registered office or at any other location approved in advance by the Bank in consultation with the FSMA.

Thus, companies that intend to use cloud service providers for the retention of the aforementioned documents should comply not only with the rules of this Circular, but also with the additional rules developed by the Bank for the retention of insurance documents.

2. Documentation and reporting to the Bank

2.1. Internal documentation

As indicated in point 7.6. of the overarching circular on governance, outsourcing companies are advised to keep a register with information on all their outsourcing arrangements (whether critical/important or not). More specifically for cloud outsourcing, the company is advised to keep records of these arrangements in

this register (which should be updated on a regular basis). It is also recommended that the company keep records of terminated cloud outsourcing arrangements for an appropriate retention period. At the Bank's request, the company should provide it with all the information necessary to enable it to ensure the supervision of the company, including a copy of the outsourcing agreement.

2.2. Reporting to the Bank

The general reporting obligations in relation to outsourcing are specified in Section 7.6. of the overarching circular on governance.

2.2.1. List of critical or important outsourcings

Cloud outsourcings that are considered critical or important should be included in the list of critical or important outsourcings to be submitted to the Bank on an ongoing basis through the eCorporate platform (reporting B.9 as mentioned in the eCorporate Communication).

For cloud outsourcings that are considered critical or important, this list should include the same information as for all other cases of critical or important outsourcings (cf. Section 7.6. of the overarching circular on governance). However, the following additional information should also be mentioned:

(i) the fact that the outsourcing is to cloud services;
(ii) the date of the most recent risk assessment and a brief summary of the main results;
(iii) the dates of the most recent and next scheduled audits, where applicable;
(iv) an outcome of the assessment of the cloud service provider's substitutability (for example, easy, difficult or impossible); and
(v) whether the company has an exit strategy in case of termination by either party or disruption of services by the cloud service provider.

2.2.2. Notification to the Bank

For the prior notification to the Bank for a new critical or important cloud outsourcing, the standard form included in Annex 4 of the overarching circular on governance should be used[2]. For cloud outsourcing, several additional annexes specified in the point "Annexes - C." of that form should be submitted to the Bank.

The Bank also asks companies to notify it immediately of any material changes and/or critical incidents in relation to the cloud outsourcing. This notification can be done by updating the original form.

Furthermore, in accordance with the general outsourcing rules provided for in Chapter 7 of the overarching circular on governance, it should be specified that the notification file to be submitted to the Bank for an important or critical cloud outsourcing should systematically be accompanied by an opinion of the person responsible for the compliance function confirming compliance with the governance rules on outsourcing and the completeness of the notification submitted (cf. Annex 5 of the overarching circular on governance).

3. Date of application

This Circular applies from 1 January 2021. This implies that from that date, all outsourcings entered into, renewed or amended by insurance or reinsurance companies should comply with this Circular.

For existing and current cloud outsourcings related to critical or important functions or activities, companies have until 31 December 2022 to comply with the Circular[3]. Until that date, these outsourcings remain

2 If a cloud outsourcing that was not originally considered critical or important becomes so after a while, the insurance company should immediately inform the Bank and provide it with the standard form included in Annex 1.

3 If the review of cloud outsourcing agreements relating to critical or important operational functions or activities is not finalised by 31 December 2022, the company should immediately inform the Bank of that fact and set out the measures planned to complete the review or the possible exit strategy. Where appropriate, the Bank may agree with the company on an extended timeline for completing this review. For the review of existing and current cloud outsourcings that are not related to critical or important

subject to Communication NBB_2012_11 on prudential expectations regarding cloud computing. This Circular will thus definitively repeal Communication NBB_2012_11 on prudential expectations regarding cloud computing from 1 January 2023.

A copy of this Circular is being sent to the accredited statutory auditor(s) of your company.

Yours faithfully,

Pierre WUNSCH
Governor

functions or activities, the company should inform the Bank by 31 December 2022 whether or not it intends to bring these outsourcings in line with the EIOPA Guidelines.