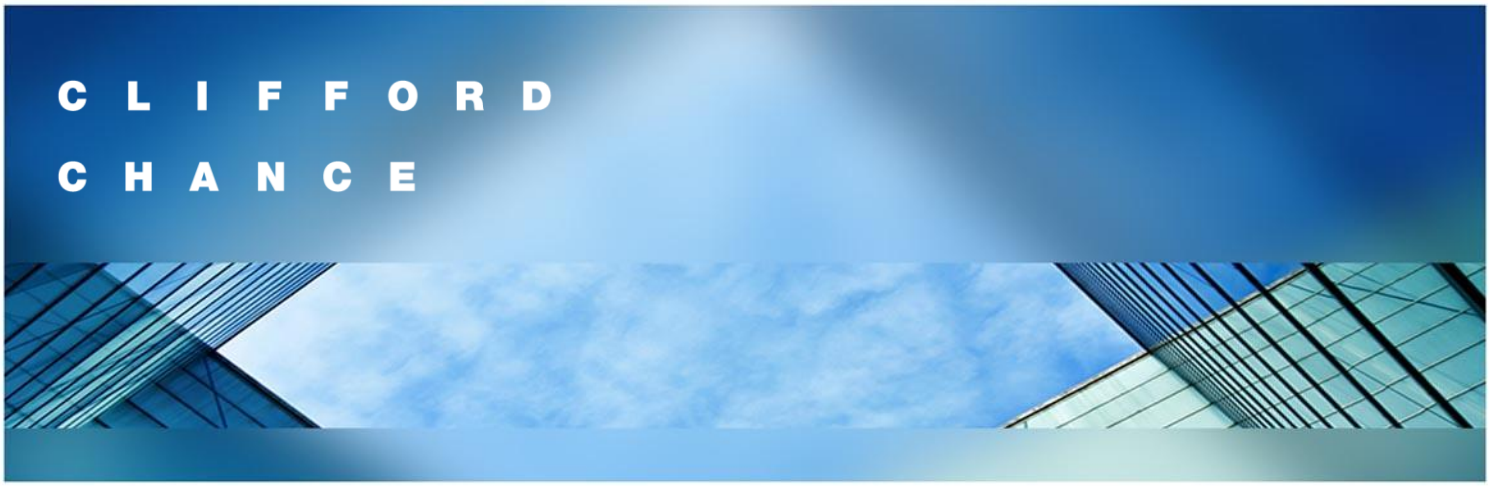

LUXEMBOURG INSURANCE REGULATOR CAA AMENDS CLOUD OUTSOURCING RULES

On 5 August 2021, the Luxembourg insurance supervisory authority Commissariat aux Assurances ("**CAA**") adopted a new Circular Letter 21/15 on outsourcing to cloud computing service providers (the "**Cloud Circular**") that applies to CAA supervised insurance and reinsurance undertakings.

More than a year ago, the CAA had already issued a circular letter (20/13) which merely informed of the full application by the CAA of the EIOPA Guidelines on outsourcing to cloud service providers (EIOPA-BoS-20-002) (the "**Guidelines**") and remembered (re-)insurance undertakings of their professional confidentiality ('insurance secrecy') obligations. The new Cloud Circular adopts the Guidelines by setting them out in the text of the Cloud Circular and integrates certain additional requirements of the CAA in it. The additional requirements relate to the setting up of an information security function, local expertise and competencies, the content of contracts and the related compliance assessment, the content of the cloud outsourcing notification to the CAA, insurance secrecy related aspects and the documentation in case of service interruptions.

This briefing is aimed at providing an overview of these CAA specific requirements that are additional to or further specifying the Guidelines and other legal or regulatory requirements relevant in this context. This briefing does not deal with the Guidelines themselves or such further legal or regulatory requirements.

INFORMATION SECURITY FUNCTION

The Cloud Circular requires that (re-)insurance undertakings appoint a person to be responsible for the use of cloud services and to be the guarantor for the competencies of the personnel managing the cloud service resources. Such

Key aspects

- The Cloud Circular is aimed at adding further specifications and requirements to the existing implementation of the EIOPA Guidelines on outsourcing to cloud service providers by the CAA in Luxembourg and is applicable to CAA supervised (re)insurance undertakings.
- These additional requirements relate to the setting up of an information security function, local expertise and competencies, contract content and related compliance assessment, the content of the cloud outsourcing notification to the CAA, insurance secrecy related aspects, and the documentation of service interruptions.
- The Cloud Circular applies from 1 November 2021 to all cloud outsourcing agreements concluded or amended as from this date.
- By 31 December 2022 (re)insurance undertakings shall have revised and amended pre-existing cloud outsourcing agreements related to critical or important functions to comply with the Cloud Circular.

person has to be qualified and have command of the impacts of the outsourcing to the cloud service provider.

The appointed person may also be exercising other functions and in principle needs to be an employee of the Luxembourg (re)insurance undertaking. The undertaking may however appoint a person of a group entity, provided such person is hierarchically linked to the authorized manager (*dirigeant agréé*) of the (re)insurance undertaking.

LOCAL EXPERTISE AND COMPETENCIES

It is required that concerned undertakings keep the necessary expertise to efficiently control the performances and tasks that are outsourced to the cloud service provider and the management of the outsourcing related risks.

Furthermore, concerned undertakings have to ascertain that the personnel in charge of the management of the cloud service resources, of internal audit and of the information security function dispose of sufficient competencies to ensure the fulfilment of their functions, on the basis of appropriate training on the management and the security of the cloud services specific to the cloud service provider. The information security function is responsible for the implementation of this requirement.

CONTRACTUAL REQUIREMENTS

The Cloud Circular provides that the cloud services agreement relating to the outsourcing of critical or important operational functions or activities must be submitted to the law and jurisdiction of a Member State of the European Union ("**EU**"), preferably of the Grand Duchy of Luxembourg. Where however the agreement is a group contract permitting the Luxembourg undertaking as well as other group entities to benefit from the cloud services, the agreement may be submitted to the law of the country of the group entity that is executing the agreement. Where such law is a law of a third country to the EU, the Cloud Circular requires however that the rules for outsourcing to cloud service providers have to be equivalent to those in the European Union. The relevant undertaking is obliged to determine whether the rules of the third country are equivalent. The correlation table that has to be produced as part of the compliance assessment by the undertaking (see further above) needs to be completed in such case by the rules and guidelines relating to outsourcing to cloud services providers applicable in the third country of the group entity executing the agreement.

The Cloud Circular also provides for specific rules in relation to the resilience structure to be agreed upon in a cloud services agreement relating to the outsourcing of critical or important operational functions or activities, the general rule being that the parties need to agree upon a resilience of the outsourced cloud services in the EU. The Cloud Circular contains further rules for cases where processing, data and systems are divided over different data centres in the world or cases of group contracts with group entities outside of the EU.

As regards the contractual requirements set out in the paragraphs above, the relevant undertaking must notify the CAA where such requirements cannot be complied with. Such notification must include a detailed argumentation justifying why the relevant cloud service provider was selected and indicating the resilience measures envisaged in case of default of the service provider or failure of communications permitting access thereto.

The Cloud Circular finally requires, on top of the rules foreseen in the Guidelines and without prejudice to Article 274 of the Commission Delegated Regulation (EU) 2015/35 (the "**Delegated Regulation**"), that the agreement with the cloud service provider relating to the outsourcing of critical or important operational functions or activities must also include provisions

regarding the termination thereof for which case the cloud service provider must commit to permanently delete the data and systems outsourced within a reasonable timeframe (without prejudice to applicable legal provisions).

SELF ASSESSMENT WITH CORRELATION TABLE

As part of the assessments that (re)insurance undertakings need to carry out in relation to the cloud outsourcing, the Cloud Circular imposes on them to carry out and document a self-assessment on the compliance of the outsourcing contract with the Cloud Circular, Article 274 of the Delegated Regulation and the EIOPA Guidelines on System of Governance (EIOPA-BoS-14/253) (the "**Governance Guidelines**"). The documentation has to comprise a correlation table (*table de correspondance*) detailing the compliance with these regulatory texts.

CLOUD OUTSOURCING NOTIFICATION TO THE CAA

The Cloud Circular refers in respect of the notification duties of a (re)insurance undertaking for a cloud outsourcing arrangement to the CAA to the general rules applicable to outsourcing notification under the Luxembourg law of 7 December 2015 on the insurance sector (as amended) (the **"ISL**") as further specific by the Governance Guidelines. In addition to adopting the minimum content requirements under these rules and the Guidelines, the CAA adds as additional points that (re)insurance undertakings need to provide the CAA with a description of the expected operational and financial benefits for the undertaking itself as well as those expected for the parties concerned by the insurance contracts, i.e. the insurance policyholder, the insured person and the insurance beneficiary ("**Concerned Insurance Parties**").

INSURANCE SECRECY

Insurance undertakings and, to a limited extent, reinsurance undertakings supervised by the CAA are subject to the statutory insurance secrecy obligation provided for in Article 300 of the ISL. To the extent they are subject to insurance secrecy and the outsourcing to a cloud outsourcing provider comprises personal data of the Concerned Insurance Parties or permitting to identify Concerned Insurance Parties, these undertakings must:

(i) perform a legal analysis in order to determine whether it is necessary that the policyholder has accepted the outsourcing in accordance with the terms provided for in Article 300(2*bis*) of the ISL (the CAA notes here that in absence of court decisions on the form of such consent, it is not excluded that certain Concerned Insurance Parties may be able to contest the validity of their consent in court);

(ii) document and regularly update the analysis referred to under (i), depending on certain changes or developments further set out in the Cloud Circular, including as regards case law;

(iii) ascertain that the personnel working for the cloud service provider can in no case access to personal data of Concerned Insurance Parties and to the systems that the Luxembourg undertaking holds on the cloud infrastructure, without having obtained prior explicit consent by such undertaking and without a surveillance mechanism is put at the disposal of the undertaking so that it can control the access so obtained. It is being noted that such access shall remain exceptional. In specific circumstances of legal obligations or extreme emergency situations due to technical incidents requiring immediate access, *ex post* information of the Luxembourg undertaking of the access may be permitted in which case certain further conditions apply;

(iv) verify that the access of the cloud service provider is restricted and limited by preventive and detective measures that are in line with good security practices and are audited at least annually; and

(v) ensure that sufficient protective measures are taken to prevent unauthorized persons from gaining access to their systems. In particular, the relevant entity must provide for telecommunications to be encrypted or still protected using other technical means available to ensure the security of communications.

These requirements are without prejudice and need to be read in conjunction with additional personal data protection rules and requirements of the EU General Data Protection Regulation (GDPR) and of the competent authority for GDPR matters, being in Luxembourg the National Data Protection Commission CNPD.

DOCUMENTATION IN CASE OF SERVICES INTERRUPTION AND CONSUMER PROTECTION

In case there is an interruption of outsourced services provision as a result of the default of the service provider for more than a day, the undertaking has to document in a register certain aspects related to such a default (such as its duration and nature, its impacts on clients of the undertaking, the number of affected clients, client information and compensation measures, impacts on the undertaking itself or remediation measures). The register needs to be made available to the CAA on request and the outsourcing to a cloud service provider shall in no case be implemented to the detriment of the quality of the services provided to the clients of the undertaking.

Additionally, the undertaking's administrative, management or supervisory body needs to be informed periodically not only of identified risks, as it is foreseen in the Guidelines, but also of the service provider defaults observed during the period reported on.

RELATIONSHIP WITH CIRCULAR LETTER 20/13

The Cloud Circular finally does not abolish the previous circular letter 20/13 that already in the past fully adopted and applied the Guidelines. As per the wording of the Cloud Circular title, the former circular is merely amended and supplemented. The few topics not touched upon explicitly in the Cloud Circular but that are contained in the Guidelines, such as the proportionality principle or the *mutatis mutandis* application of the Guidelines to groups, should therefore still be of relevance.

ENTRY INTO FORCE AND APPLICATION

The Cloud Circular applies from 1st November 2021 to all cloud outsourcing agreements concluded or amended from this date.

(Re)insurance undertakings must further revise and amend existing cloud outsourcing agreements relating to critical or important operational functions or activities so that these agreements comply with the Cloud Circular on 31 December 2022 at the latest.

Where such a revision and amendment is not implemented by 31 December 2022 by an undertaking, it has to inform the CAA and indicate the measures taken to finalize the revision or, as the case may be, the exit strategy.

CLIFFORD
CHANCE

CONTACTS

Udo Prinz
Counsel

T +352 48 50 50 232
E udo.prinz
@cliffordchance.com

Yolanda Ghita-Blujdescu
Senior Associate

T +352 661 48 52 26
E yolanda.ghita-blujdescu@cliffordchance.com