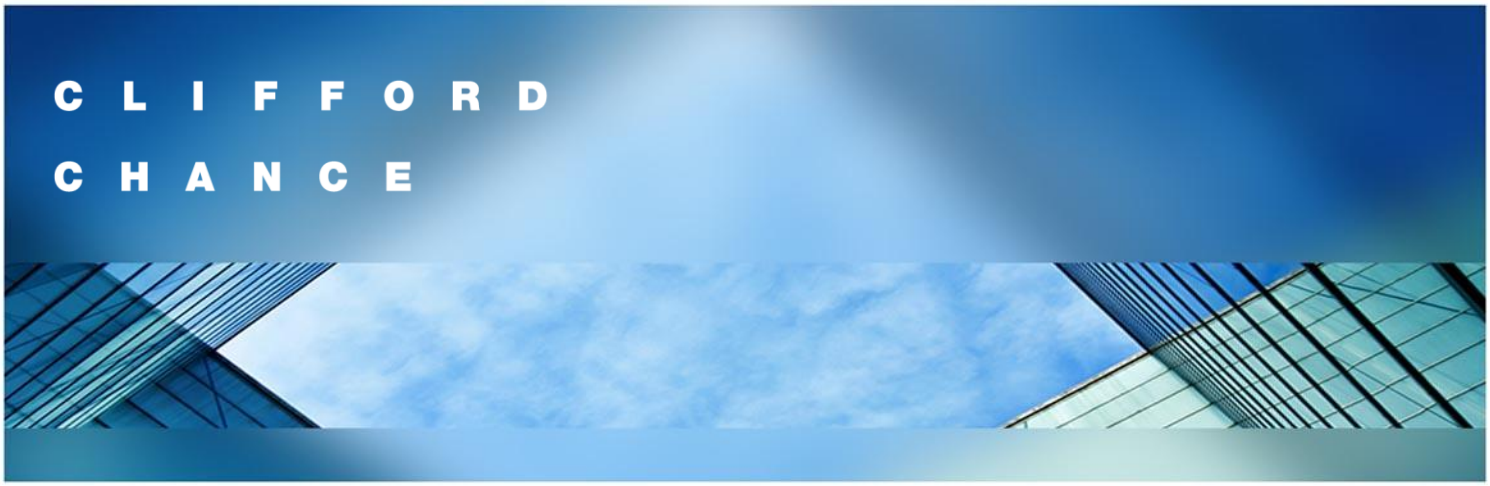

LUXEMBOURG FINANCIAL SECTOR REGULATOR DEFINES REQUIREMENTS FOR SUPERVISED ENTITIES USING TELEWORKING.

On 9 April 2021, the Luxembourg's financial sector regulator (the "**CSSF**") published a new circular (Circular CSSF 21/769 - the "**Circular**") on governance and security requirements for supervised entities to perform tasks or activities through telework (or remote working). The Circular aims at clarifying how employers in the financial sector can safeguard their substance and IT system security while their employees are working remotely.

CONTEXT

New framework for remote working

In order to counter the risks of the current health crisis, coupled with the possibilities afforded through the use of new technologies, employers rely more and more on 'teleworking' or 'remote working' arrangements, whereby employees are allowed and enabled to work outside of their employer's premises (namely from home).

To respond to this increasing reliance on remote working, new frameworks were adopted in Luxembourg.

On 20 October 2020, an agreement has been reached between the employers' representatives and the labour unions regarding teleworking which has been declared generally applicable (*d'obligation générale*) in Luxembourg as from 2 February 2021 (the "**Convention**").

With this new Circular, the CSSF defines governance and security requirements for supervised entities implementing and using work processes based on telework solutions.

Scope and applicability of the Circular

The Circular applies to all entities under the supervision of the CSSF, including not only credit institutions, but also undertakings for collective investments and their management companies, investment firms, specialised professionals of the financial sector, administrative agents or other support professionals, etc. It also applies to branches (in Luxembourg or abroad) of Luxembourg-based entities, as well as Luxembourg branches of foreign entities. Insurance sector entities are not supervised by the CSSF, but by the

Key issues

- The Circular CSSF 21/769 details governance and IT requirements when staff of supervised entities works remotely.
- The Circular applies to all entities under the supervision of the CSSF and includes their foreign branches.
- The CSSF's approval is not required in order to implement telework solutions.
- Supervised entities must retain their central administration and sufficient substance at their Luxembourg premises, in order to promptly deal with time-sensitive issues and should assess to what extent it allows its staff members to work remotely.
- Supervised entities must put in place appropriate internal organisation and control (e.g. risk management, telework policy, monitoring) and address ICT and security risks.
- Telework is organised under the ultimate responsibility of the Board of Directors of the supervised entity (or any other body that represents the supervised entity).
- The Circular applies under normal general working conditions and outside the COVID-19 pandemic.

Commissariat aux Assurances (CAA). They are hence outside the scope of the Circular.

The Circular is meant to apply in "normal general working conditions" and excludes temporary remote working arrangements intended to address risks related to the COVID-19 pandemic (in relation to which the CSSF has already provided specific guidance in its FAQ-COVID-19 N°1 of 3 March 2020 and a preceding press release of 2 March 2020). It does not apply under pandemic situations or in case of other exceptional circumstance having a comparable impact on the general working conditions.

The Circular does not create any rights or precedence for employees to claim a right to telework and applies without prejudice to the Convention which sets out the general framework applicable to telework. Accordingly, remote working must be performed on a voluntary basis (i.e., at the employee's request and based on a prior approval by the employer), irrespective of whether the remote working is made on an occasional or regular basis. The definition however excludes forms of remote access to on-premise systems (while on a business trip, attending conferences, etc.). It also excludes the access to external systems while within the employer's premises.

The scope of the Circular is also limited to the remote working of staff members, defined as all employees of the supervised entity, including persons at its disposal through a contract with a third-party employer (e.g., secondees).

The Circular will enter into force at the earliest on 30 September 2021 or at the end of the COVID-19 pandemic (most probably once the exceptional measures implemented to respond to the COVID-19 crisis will have been lifted).

KEY TAKEAWAYS

By defining the minimum requirements with respect to telework, the CSSF wants to make sure that supervised entities maintain at all times a robust central administration (i.e. a decision-making centre and an administrative centre) as well as sufficient substance at its premises in Luxembourg. Such requirements namely relate to governance and IT security.

Substance and governance requirements

The Circular provides for a framework relating to internal organisation and internal control supposed to address substance and governance requirements, notably:

- performing an assessment of the risks in implementing teleworking and identifying appropriate mitigation measures;
- implementing a telework policy setting the framework and the limits under which telework may be allowed and which shall cover a number of items listed in the Circular;
- monitoring the compliance with the Circular and the telework policy;
- having sufficient staff to ensure the continuation of critical activities and make sure that the staff members shall be able to return to premises on short notice in case of need;
- having at least one authorised manager on-site at all times; and

- including telework related processes and procedures and the telework policy within the controls conducted by the internal control functions (i.e. compliance, risk management, information security and internal audit).

It is worth noting that telework is organised under the ultimate responsibility of the Board of Directors of the supervised entity (or any other body that represents the supervised entity).

An approval of the CSSF is not necessary prior to the implementation of remote working arrangements.

IT security requirements

The CSSF requires supervised entities to ensure that ICT and security conditions under which they authorise their employees to telework are proportional to the risks to which they are (or could be) exposed.

This can be achieved through the following organisational measures:

- defining the high-level principles and rules applicable in the context of telework in the supervised entity's security policy;
- reviewing and adapting the access rights management procedures and the accesses granted for telework;
- providing adequate training to staff members and promote best practices;
- favouring the use of corporate owned devices which are under the full control of the supervised entity (i.e. over private devices which are not considered as secure) and ensuring that where data can be stored on the device, the storage media is encrypted;
- maintaining over time a high level of security and availability of the telework infrastructure;
- ensuring the security of connections (e.g. implementation of a 2-factor authentication) for any connection by an employee working remotely. A dynamic 2-factor authentication, such as an external device generating temporary codes (e.g. a one-time password token), is required in case of connections with access to data related to critical activities.

Data protection issues

Remote working entails the processing of personal data, requiring justification under the General Data Protection Regulation (EU 2016/679) ("**GDPR**"), as well as the possible monitoring of employees, subject to specific formalities under the Luxembourg Labour Code.

Given that remote working exposes supervised entities to further risks of confidentiality and personal data breaches, a review of the supervised entities' reporting obligations in case of such incidents under applicable laws and regulations (such as the GDPR) is recommended.

CONCLUSION

Supervised entities are required to draw up or review their remote working policies in light of the recently published Circular, and also to assess possible gaps with applicable laws and regulations. Our dedicated specialists teams are available to advise and assist you from relevant legal perspectives in

relation to complying with the requirements of the Circular, such as requirements for risk assessment performance, drafting or reviewing of telework policies or security policies, and advise more generally on the legal, tax, regulatory and contractual aspects relevant in the context of implementing teleworking solutions.

Generally, the CSSF draws the attention of supervised entities that they need to comply with mandatory public order provisions. Particular attention should be paid to labour and tax law, as well as company law, professional secrecy, and social security requirements. The CSSF expects supervised entities to give due consideration to these laws when implementing telework, especially for non-resident staff members. Each supervised entity also must comply with European and national regulations regarding freedom of establishment and freedom to provide services when deploying teleworking in a cross-border context.

Careful consideration should also be given to the application of remote working arrangements for branches of supervised entities located abroad, as remote working may be subject to local laws and regulations, including employment law.

CLIFFORD
CHANCE

CONTACTS

Albert Moro
Partner

T +35 485050 204
E albert.moro
@cliffordchance.com

Udo Prinz
Counsel

T +35 485050 232
E udo.prinz
@cliffordchance.com

Ada Schmitt
Senior Associate

T +35 485050 435
E ada.schmitt
@cliffordchance.com

Charles-Henri Laevens
Senior Associate

T +35 485050 485
E charleshenri.laevens
@cliffordchance.com

Boika Deleva
Associate

T +35 485050 260
E boika.deleva
@cliffordchance.com

Ottavio Covolo
Associate

T +35 485050 221
E Ottavio.covolo
@cliffordchance.com

Elisabeth Franssen
Associate

T +35 485050 264
E elisabeth.franssen
@cliffordchance.com