

## CSSF circular on governance and security requirements for teleworking



On 9 April 2021, the Commission de Surveillance du Secteur Financier (the « CSSF »), the Luxembourg financial supervisory authority, adopted a circular 20/769 on governance and security requirements for supervised entities to perform tasks or activities through telework (the “Circular”). The Circular enters into force on 30 September 2021 and does not apply under pandemic situations or in case of other exceptional circumstances having a comparable impact on the general working conditions. The Circular applies to all supervised entities, including their branches.

The Circular defines when a work relationship may be qualified as telework, i.e. when the following cumulative criteria are met:

- work must be delivered by means of information and communication technologies based on a previous approval by the employer;
- work must be performed on a regular or occasional basis and voluntary basis and within the defined working hours at a predetermined place which is different from the employer’s premises.

The Circular sets out baseline requirements such as:

- the supervised entities are required to maintain at all times a robust central administration in Luxembourg, meaning i.a. that staff should be able to return to the supervised entity’s premises on short notice in case of need;
- the amount of normal working time that staff is allowed to telework should be limited;
- in principle, at least, one authorised manager shall be on-site at the head office at all times;
- the head office remains the decision-making center;
- the ongoing performance of critical activities shall be guaranteed.

Furthermore, a telework policy should be implemented and compliance thereof should be monitored. Evidence of such monitoring should be maintained in order to also demonstrate compliance with the requirements of the Circular to independent auditors and to the CSSF. Internal control functions should include the review of the telework policy, process flows and compliance with the legal and regulatory requirements in their respective pluri-annual work program.

In terms of security risks and information and communication technology systems (“ICT”), the security policy of supervised entities shall be adapted to define high-level principles and rules

applicable in the context of telework to protect the confidentiality, integrity and availability of entities' data and ICT systems. The supervised entity shall also ensure that it keeps control over the security of the devices used by the users to connect remotely to the ICT systems which can be best achieved by using corporate owned devices rather than private devices. The supervised entity also shall maintain over time a high level of security and availability of the telework infrastructure. It furthermore has to ensure that data in transit is secured. A two-factor authentication has to be implemented when connecting remotely to the systems of the supervised entity. Finally, the supervised entity shall review the security of the communication chain and have a solid monitoring process.

The Circular will thus impact the internal organisation and infrastructure of supervised entities which will need to adapt to the above. We may assist you in ensuring compliance with the requirements set out under the Circular by reviewing your organisation and processes, implementing or adapting current policies and procedures and answering any questions you may have. To that effect, please do not hesitate to contact one of our experts.

[Aurélia Viémont](#), Senior Counsel | Avocat à la Cour

[Aurélien Hollard](#), Partner | Avocat à la Cour

[Benjamin Bada](#), Partner | Avocat à la Cour

[Sarah Hantscher](#), Managing Associate | Avocat