cssf

Commission de Surveillance
du Secteur Financier

Circular CSSF 21/769

Governance and security requirements for Supervised Entities to perform tasks or activities through Telework

Commission de Surveillance du Secteur Financier

Circular CSSF 21/769

RE: Governance and security requirements for Supervised Entities to perform tasks or activities through Telework

Luxembourg, 9 April 2021

To all Supervised Entities

Ladies and Gentleman,

The present circular defines the governance and security requirements with respect to the implementation and utilisation by an entity under the supervision of the CSSF of work processes based on Telework solutions.

It contributes to the sound and prudent management, the proper organisation of these Supervised Entities and the preservation of information security by providing guidance on the requirements the Supervised Entities have to comply with.

No approval by the CSSF is required in order to implement, maintain or extend Telework solutions for staff in a Supervised Entity.

This circular applies under normal general working conditions. It does not apply under pandemic situations (for example COVID-19) or in case of other exceptional circumstances having a comparable impact on the general working conditions.

This circular is limited to financial sector regulatory requirements. All contractual relations between Supervised Entities and their employees are out of scope of the present circular. It does not create any precedence for rights or obligations on whether Telework may be implemented by entities under the supervision of the CSSF. Furthermore, this circular does not interfere in any legal provisions that are part of the mandatory public policy provisions (*règles d'ordre public*) or part of the Luxembourg Labour Code. It is intended solely to provide additional guidance on the governance and security requirements to be followed when implementing Telework solutions for employees of entities supervised by the CSSF.

Commission de Surveillance du Secteur Financier

TABLE OF CONTENTS

Commission de Surveillance du Secteur Financier

I. Scope

1. This circular applies to all Supervised Entities, hereinafter collectively referred to as "**Supervised Entities**" or individually as "**Supervised Entity**", including their branches in Luxembourg or abroad, to the extent that Telework is authorised in the countries where the branches are established and they comply with national regulations. In this context, specific requirements stated in this circular apply as minimum standards to be adopted by branches of Supervised Entities.

2. This circular also applies to Luxembourg branches of entities originating from outside the European Economic Area.

3. Luxembourg branches of entities originating from a Member State of the European Economic Area may also use Telework in accordance with the requirements provided for in this circular, in case Telework is authorised in their home country. These branches and their head offices shall ensure that the use of Telework by the Luxembourg based branches also complies with all national rules and regulations applicable in the home Member State.

II. Definitions

Telework

4. Telework is a form of organising and/or carrying out work, using information and communication technologies within the framework of an employment contract authorising work, which would ordinarily be carried out in the employer's premises, to be performed outside the premises of the employer.

5. The following cumulative criteria must be met so that a work relationship may be qualified as Telework:

   a. Work must be delivered by means of information and communication technologies based on a previous approval by the employer;

   b. Work must be performed on a regular or occasional and voluntary basis and within the defined working hours at a predetermined place that is different from the employer's premises. Supervised Entities shall have rules in place to define from where Telework is allowed. These rules need to be documented and respected.

6. It should be noted that other forms of remote access by staff members of the Supervised Entities (i.e. while on business trip, e.g. client relationship managers, when attending conferences or professional training), as well as connections from the employer's premises to systems not hosted in the employer's premises are not covered in the scope of this circular.

Commission de Surveillance du Secteur Financier

7. For the avoidance of doubt, work performed by staff members of the Supervised Entities in a location other than the premises of the employer, in the context of the activation of a Disaster Recovery Plan/ Business Continuity Plan, does not qualify as Telework and, consequently, does not fall under the scope of this circular.

Staff or staff member

8. Staff or staff member means all employees of Supervised Entities including key functions and authorised management. Persons put at the disposal of a Supervised Entity through a contract by a third-party employer are also considered staff members.

9. For the purposes of this circular, a staff member who is teleworking is a "Teleworker".

Employer's premises or premises

10. The employer's premises include the head office and any additional premises in Luxembourg that Supervised Entities use as well as, in the case of branches, the premises of branches of Supervised Entities or Luxembourg branches of entities.

Privileged users

11. Privileged users are users with access rights enabling them to carry out sensitive operations, both for ICT operations (e.g. system administrators) and for business operations. These sensitive operations are typically related to the provision of critical activities.

Critical activities

12. Critical activities are activities in respect of which the occurrence of a problem may have a significant impact on the Supervised Entity's ability to meet the regulatory requirements or even to continue its activities (e.g. transaction processing, order input/upload, 4-eye validations, remote administrative access to ICT systems by the ICT team, etc.).

Authorised Management

13. Authorised Management means persons authorised by the CSSF for day-to-day management or persons authorised by the CSSF to effectively conduct the business of a supervised entity.

Commission de Surveillance du Secteur Financier

III. General principles

14. Supervised Entities are required to maintain, at all times, a robust central administration in Luxembourg and to maintain sufficient substance in its premises, also in order to allow them to deal with emergencies and other time-critical issues in due time. Nevertheless, Supervised Entities may allow staff to perform tasks and activities through Telework. In principle, all staff, regardless of its function, may be allowed to telework within the limits set in the present circular in order to guarantee adequate governance of the Supervised Entities and subject to the legal and regulatory framework on Telework in place. The present circular does not create any precedence for rights or obligations on whether Telework may be implemented by entities under the supervision of the CSSF. Furthermore, all contractual relations between Supervised Entities and their employees are out of scope of the present circular.

15. Each Supervised Entity should assess to what extent it allows its staff members to work remotely. This assessment should consider the risks of Telework and define limits within which it might be allowed to perform tasks remotely. In particular, smaller Supervised Entities with a limited number of staff may need to adapt their internal organisation, taking into consideration requirements, relative to their size.

16. Telework shall, in no case, jeopardise the regular operational functioning of a Supervised Entity. It shall be sufficiently robust to ensure that the entity's activities continue in an effective and secure manner and that all elements of the entity's internal control framework remain operational without exception and on an ongoing basis. The Supervised Entity has to protect, at all times, even in the context of Telework, the confidentiality, integrity and availability of the entity's data and information systems.

17. Telework is organised under the ultimate responsibility of the Board of Directors of the Supervised Entity or any body that represents the Supervised Entity, by virtue of the law and of the instruments of incorporation.

18. An approval by the CSSF is not required in order to implement Telework.

IV. Compliance with other legal provisions

19. The use of Telework by Supervised Entities may not contravene any legal provisions that are part of the mandatory public policy provisions (*règles d'ordre public*) and shall, in particular, comply with the provisions of the Luxembourg Labour Code.

20. In addition, Supervised Entities shall take into account that the prudential requirements with respect to substance and central administration may differ from other legal provisions, especially laws and regulations relating to tax

(domestic, foreign and international), companies, professional secrecy, data protection and social security. The CSSF expects Supervised Entities to give due consideration to these laws when implementing Telework, especially in the context of Telework by non-resident staff members. The present circular may not be interpreted in a way that Supervised Entities may circumvent laws and regulations in place.

21. Each Supervised Entity shall also comply with European and national regulations regarding freedom of establishment and freedom to provide services when deploying Telework.

22. This circular does not create any precedence for rights or obligations on whether Telework may be implemented by entities under the supervision of the CSSF. All contractual relations between Supervised Entities and their employees are out of scope of the present circular.

V. Baseline requirements

23. A robust central administration consists of a "decision-making centre" and an "administrative centre", which includes sufficient staff with the necessary skills, knowledge and expertise as well as the technical and administrative infrastructure, to exercise its function or activity.

24. In order to comply with this central administration requirement, the staff members shall be able to return to the Supervised Entity's premises on short notice in case of need.

25. In the case of branches of Supervised Entities located outside of Luxembourg, it also has to be ensured that staff may return to the branches' premises on short notice in case of need.

26. It is the responsibility of the Board of Directors of the Supervised Entity or any body that represents the Supervised Entity, by virtue of the law and of the instruments of incorporation, to define, in advance, the extent to which Telework may be used without violating central administration requirements in accordance with applicable laws and regulations.

27. As a baseline, the following specific criteria shall be respected when implementing, using or extending Telework:

    a. The number of staff of a Supervised Entity which may telework at the same time must comply with central administration requirements.

    b. The amount of normal working time, individual staff members are allowed to telework, should be limited.

    c. In principle, at least 1 authorised manager shall be on site at the head office at all times. Furthermore, key functions shall be sufficiently represented every day in the premises and permanently guarantee the

adequate functioning of the activities and controls as well as proper decision-taking. For this purpose, Supervised Entities shall take into account the size and organisation of the Supervised Entity and the nature, scale and complexity of its activities.

d. The Supervised Entity shall be able to demonstrate that the head office remains at all times the "decision-making centre" as part of the central administration of the Supervised Entity.

e. The CSSF reminds the Supervised Entities that, in particular, the ongoing performance of critical activities shall be guaranteed. This aspect shall therefore be adequately considered in the implementation of Telework and the related policy.

   i. As such, the Supervised Entities shall ensure that interruptions of Telework (e.g. connection disruption) do not have a substantial impact on the entities' capacity to carry out their activities in an adequate, timely and secure manner.

   ii. Provisions shall be made by the Supervised Entities to ensure that critical activities can be covered by a sufficiently skilled and responsible staff member present on site at the entity's premises to guarantee the adequate functioning of the activities and controls during business hours.

VI. Internal organisation and internal control framework

Risk management

28. The Supervised Entity shall perform a risk analysis in order to identify the inherent risks in implementing Telework, in particular, the operational risks, including legal, Information and Communication Technology (ICT), compliance and reputational risks.

29. Particular attention should be paid to:

   a. The evaluation of aspects related to labour law and tax law (including permanent establishment issues), as well as company law and social security requirements;

   b. The risk associated with the Telework of privileged users;

   c. The respect of the professional secrecy and data protection requirements (e.g. when professional devices or documents may leave the secure professional environment).

30. Supervised Entities shall ensure the implementation of the necessary mitigating controls and measures to keep the residual risks within the

acceptable limits according to the entities' risk appetite. Risk identification and mitigation measures should be adequately formalised.

31. Supervised Entities should regularly review their risk analysis and the appropriateness of the implemented mitigating measures, considering lessons learned, potential changes in the organisation, or their environment, working processes or Telework technical architecture as well as emerging threats such as e.g. cybercrime or opportunistic attacks around the Telework context.

Telework policy

32. The Board of Directors of the Supervised Entity or any body that represents the Supervised Entity, by virtue of the law and of the instruments of incorporation, shall define a Telework policy setting the framework and the limits under which Telework may be allowed. This policy shall clearly determine:

    a. Business units or departments that may use Telework and activities and/or functions that may be performed via Telework;

    b. Functions and/or activities of business units or departments that must always be performed on site in the premises of the Supervised Entity;

    c. Minimum number of staff required to work at the same time at the premises in Luxembourg at entity level and, where relevant, at business unit or department levels;

    d. Working hours within which Telework is allowed;

    e. Control procedures that have to be implemented in order to be able to monitor the proper execution of work performed by the staff through Telework;

    f. Minimum physical meetings that should be held at the head office in Luxembourg;

    g. Measures to be taken in order to ensure that risks remain contained, including compliance with confidentiality and data protection regulations.

33. The policy shall set the operational framework enabling the Authorised Management to monitor the number of staff members who are effectively teleworking.

34. The existing management information system and control environment of a Supervised Entity cannot be altered while allowing tasks to be performed via Telework. Existing controls (e.g. 4-eye controls), dashboards and reporting need to be executed in the same way and with the same frequency as defined in the existing internal procedures of the Supervised Entity.

35. The Board of Directors of the Supervised Entity or any body that represents the Supervised Entity, by virtue of the law and of the instruments of incorporation, shall review the Telework policy annually based on the updated risk analysis and its operational and management objectives.

Monitoring of the use of Telework

36. The CSSF monitors compliance with this circular. To that effect, the Supervised Entity shall maintain the evidence enabling the monitoring of the compliance with the Telework policy (e.g. record the name, function and department/unit of each staff member teleworking). This should also allow demonstrating the compliance with the present requirements to independent auditors and to the CSSF. The Supervised Entity should, upon request, make available to the CSSF either the full evidence mentioned in the preceding sentence, or relevant parts thereof allowing demonstration of compliance with the present requirements, in a processable electronic form (e.g. a commonly used database format). The Supervised Entity should, upon request, make available to the CSSF all information necessary to enable the CSSF to execute effective supervision of the Supervised Entity, including, where required, the Telework policy.

Controls by internal control functions over Telework

37. The internal control functions, such as (when applicable) compliance, risk management, including information security (RSSI/CISO) and internal audit, shall include the review of the Telework policy, process flows and compliance with the legal and regulatory requirements in their respective multi-year work programme and the report of any issues or findings in that regard to the CSSF in their respective annual summary reports, were applicable.

38. Furthermore, each year the annual summary reports shall, if applicable, mention any significant operational incidents in relation to Telework that might have occurred during the year. They shall also contain a short statistic on the use of Telework during the year.

VII. Requirements related to ICT and security risks

39. In principle, all paragraphs under this section apply to all Supervised Entities. When implementing these requirements, Supervised Entities should have regard to the principle of proportionality by considering the nature, scale and complexity of their activities. Risks may require higher or permit lower ICT and security measures than those described in this section. Supervised Entities remain responsible for ensuring that ICT and security conditions

under which they authorise their employees to telework are in proportion to the risks to which the Supervised Entities are or could be exposed.

Policies and procedures

40. The Supervised Entity's security policy shall define the high-level principles and rules applicable in the context of Telework, to protect the confidentiality, integrity and availability of the entity's data and information and communication technology (ICT) systems. These principles and rules can either be part of the general security policy document or be included in the Telework policy document and are, in both cases, referred to below as "Telework security policy". The Telework security policy shall be aligned with the relevant results of the risk assessment process and approved by the Board of Directors of the Supervised Entity or any body that represents the Supervised Entity, by virtue of the law and of the instruments of incorporation.
41. This Telework security policy shall be complemented at operational level by adapting or completing the existing user procedures as appropriate. Telework policies, procedures and related documents shall be updated as well as communicated to the staff members on a regular basis.

Risk awareness

42. The Supervised Entity shall ensure all staff members' awareness on risks and best practices regarding the use of Telework (e.g. through periodic training sessions, newsletters or other communications) as well as on their duties and responsibilities in line with the relevant security policies and procedures to reduce human error, theft, fraud, misuse or loss.
43. The above-mentioned awareness initiatives and/or procedures and documentation shall cover organisational and technical risks (e.g. social engineering, phishing attacks, etc.) in relation to Telework as well as the specific behaviour to be adopted by the Teleworkers.

Access rights

44. The Supervised Entity shall review and adapt its access rights management procedures and the accesses granted for Telework in line with its risk assessment and with its Telework security policy.
45. In particular, Supervised Entities should consider the need to create user roles/profiles and access rights dedicated to the Telework situation (i.e. limited compared to on-premises work), while maintaining the segregation of duties principle.

46. Access rights of Teleworkers (including of service providers) should be granted based on the "need-to-know" principle and recertified at least annually for non-privileged users and at least biannually for privileged users.

Remote access devices

47. The Supervised Entity has to ensure that it keeps control over the security of the devices used by the users to connect remotely to the Supervised Entity's ICT systems. In particular, the Supervised Entity should ensure that:

    a. When data can be stored on the device, the storage media is encrypted; the recourse to virtual desktop infrastructures, which allow avoiding storage on the device, is encouraged;

    b. The security mechanisms implemented by the Supervised Entity cannot be modified, removed or bypassed by the staff members.

48. Compliance with the above requirements can best be achieved by using company-owned devices, which are under the full control of the Supervised Entity.

49. Private devices are not considered as secure as company-owned devices; this is why they should be considered only for low-risk activities and systems. In addition, staff members carrying out critical activities shall not use private devices to carry out such activities. In particular, ICT teams shall not be able to access and administer ICT systems using private devices.

50. The potential use of privately owned devices must be considered carefully and assessed through a specific risk analysis. Despite the fact that the Supervised Entity is not the owner of the device, it must be in a position to monitor the professional data and applications that will be used on it. Solutions where the Supervised Entity installs a controlled professional environment (container) inside the private environment of the tool should allow it to keep full control over this container. Solutions based on the use of a virtual desktop infrastructure (VDI) from a privately owned device may be considered as long as the Supervised Entity is able to mitigate the risks resulting from a potentially compromised privately owned device. In addition, independent tests have to be organised on a regular basis in order to prove that either solution using a privately owned device is sufficiently secure.

51. Finally, the Supervised Entity shall ensure that the company-owned device or, if applicable, the professional container on the privately owned device can be remotely managed by a centralised management solution.

Telework infrastructure

52. The Supervised Entity shall maintain a high level of security and availability of the Telework infrastructure over time. In this context, the Supervised Entity has to ensure, at all times, that the various components are properly functioning, correctly secured and closely monitored.

53. The Supervised Entity shall implement mechanisms allowing it to detect abnormal connections and block/alert on them.

54. In particular, for the purpose of point 53, the Supervised Entity has to define a set of security and non-security criteria and requirements that have to be ensured before allowing a Teleworker to access the internal systems and data based on the risks identified during the risk assessment performed. In this context, possible criteria and requirements are (non-exhaustive list):

    a. the correct authentication of the Teleworker;

    b. the correct identification and authentication of the device;

    c. the correct identification of the remote location of the Teleworker;

    d. the connection time is within the defined working hours;

    e. the security components and mechanisms implemented by the Supervised Entity have not been modified or bypassed by the Teleworker or an attacker, are up-to-date and running.

55. Maintaining the Telework infrastructure over time implies that the Supervised Entity has a robust change management process in place, ensuring that changes do not jeopardise the implemented Telework infrastructure and security level.

Security of connections

56. The Supervised Entity has to ensure that data in transit is secured, i.e. encrypted, in accordance with its data classification and that the implemented encryption protocols (for instance IPSec, SSL), the encryption algorithm (for instance RSA, AES) as well as the chosen key size respect current leading practices.

57. A 2-Factor Authentication (2-FA) has to be implemented when connecting remotely to the systems of the Supervised Entity.

58. The implemented authentication mechanism may be adapted according to the type of operations performed remotely and the user profile (principle of proportionality).

59. For critical activities Supervised Entities are expected to implement a strong 2-FA procedure with one of the factors being dynamic (e.g. OTP).

Review of the communication chain security

60. The proper functioning of the communication chain from the remote device to the corporate infrastructure (e.g. remote access gateway) as well as the effectiveness of the implemented security measures shall be reviewed by an independent security control function (i.e. Information Security Officer, Internal Audit or specialised external third party) before the go-live of the Telework and on a regular basis thereafter.

61. In particular, this review must confirm that the implemented infrastructure, the positioning of the different security barriers and applied security and data leakage prevention mechanisms are correctly designed, tested, implemented and configured.

62. In addition, vulnerability scans/penetration tests should be organised on a regular basis, commensurate to the level of identified risk in relation to Telework.

Technology watch

63. A solid monitoring process should be in place to allow the Supervised Entity to be quickly informed of the emergence of new security vulnerabilities and to apply the necessary corrections within a short period of time. Particular attention shall be paid to the risks related to the use of privately owned devices in case their use is allowed.

Logging

64. A sound logging process shall be implemented allowing the Supervised Entity to ensure that all connections and relevant technical information related to Telework (including the connecting device used) are logged for reasons of security monitoring.

65. Access logs shall be secured to prevent unauthorised modification or deletion. The principle of proportionality shall be ensured, e.g. the granularity of logged information and the log retention period shall be proportional to the criticality of the operation carried out by the Teleworker, without prejudice to the retention requirements set out in EU and national law.

Commission de Surveillance du Secteur Financier

VIII. Entry into force, review and anti-abuse provision

66. This circular enters into force on 30 September 2021, safe exceptional circumstances as defined on page 2.

67. Based on the experience drawn from the monitoring referred to in point 36, this circular will be reviewed at the latest 12 months after its entry into force in order to address potential abuses or any other shortcomings or deficiencies.

Claude WAMPACH
Director

Marco ZWICK
Director

Jean-Pierre FABER
Director

Françoise KAUTHEN
Director

Claude MARX
Director General

Commission de Surveillance du Secteur Financier
283, route d'Arlon
L-2991 Luxembourg (+352) 26 25 1-1
direction@cssf.lu
www.cssf.lu