cssf

Commission de Surveillance
du Secteur Financier

Circulaire CSSF 21/769

Exigences en matière de gouvernance et de sécurité pour les entités surveillées en vue de l'exécution de tâches ou activités via le télétravail

Commission de Surveillance du Secteur Financier

En cas de divergence entre les textes français et anglais, le texte anglais prévaut.

Circulaire CSSF 21/769

Concerne : Exigences en matière de gouvernance et de sécurité pour les entités surveillées en vue de l'exécution de tâches ou activités via le télétravail

Luxembourg, le 9 avril 2021

À toutes les entités surveillées

Mesdames, Messieurs,

La présente circulaire a pour objet de définir les exigences en matière de gouvernance et de sécurité relatives à la mise en œuvre et à l'utilisation de processus de travail basés sur des solutions de télétravail par les entités soumises à la surveillance de la CSSF.

Elle contribue à la gestion saine et prudente et à la bonne organisation de ces entités surveillées, ainsi qu'à la préservation de la sécurité de l'information en fournissant des orientations relatives aux exigences que les entités surveillées sont tenues de respecter.

La mise en œuvre, le maintien ou l'extension des solutions de télétravail pour le personnel des entités surveillées ne requièrent pas d'autorisation de la CSSF.

La présente circulaire s'applique dans des conditions de travail générales normales. Elle ne s'applique pas en situation de pandémie (telle que la pandémie de COVID-19) ou en d'autres circonstances exceptionnelles ayant des répercussions similaires sur les conditions de travail générales.

La portée de la présente circulaire est limitée aux exigences réglementaires relevant du secteur financier. Les relations contractuelles entre les entités surveillées et leurs employés sont exclues du champ d'application de la présente circulaire. Elle ne créé pas de précédent par rapport à des droits ou obligations relatifs à la mise en œuvre du télétravail par les entités soumises à la surveillance de la CSSF. De plus, la présente circulaire ne porte pas atteinte aux dispositions légales applicables dans le cadre des règles d'ordre public ou du Code du travail luxembourgeois. Elle a uniquement vocation à fournir des orientations supplémentaires relatives aux exigences en matière de gouvernance et de sécurité à respecter lors de la mise en œuvre de solutions de télétravail pour les employés des entités soumises à la surveillance de la CSSF.

Commission de Surveillance du Secteur Financier

SOMMAIRE

Commission de Surveillance du Secteur Financier

I. Champ d'application

1. La présente circulaire s'applique à toutes les entités surveillées, ci-après dénommées collectivement « **entités surveillées** » ou individuellement « **entité surveillée** », y compris leurs succursales au Luxembourg ou à l'étranger, dans la mesure où le télétravail est autorisé dans les pays d'établissement des succursales et que ces dernières se conforment aux réglementations nationales. Dans ce contexte, les exigences spécifiques définies dans la présente circulaire font office de normes minimales à adopter par les succursales des entités surveillées.

2. La présente circulaire s'applique également aux succursales luxembourgeoises d'entités originaires d'un pays hors de l'Espace économique européen.

3. Les succursales luxembourgeoises d'entités originaires d'un État membre de l'Espace économique européen peuvent également avoir recours au télétravail conformément aux exigences prévues dans cette circulaire, si le recours au télétravail est autorisé dans leur pays d'origine. Les succursales en question et leur siège social doivent s'assurer que le recours au télétravail par les succursales basées au Luxembourg est également conforme à toutes les règles et réglementations nationales applicables dans l'État membre d'origine.

II. Définitions

Télétravail

4. Le télétravail est une forme d'organisation et/ou de réalisation du travail, utilisant les technologies de l'information et de la communication (TIC) dans le cadre d'un contrat de travail autorisant que le travail qui aurait normalement été réalisé dans les locaux de l'employeur soit effectué hors des locaux de l'employeur.

5. Les critères cumulatifs suivants doivent être respectés pour qu'une relation de travail puisse être qualifiée de télétravail :

   a. le travail doit être exécuté au moyen de technologies de l'information et de la communication sur la base d'un accord préalable de l'employeur ;

   b. le travail doit être effectué sur une base régulière ou occasionnelle et volontaire, et dans le cadre d'heures de travail définies, en un lieu prédéterminé qui est différent des locaux de l'employeur. Les entités surveillées sont tenues de mettre en place des règles définissant le(s) lieu(x) à partir duquel(desquels) le télétravail est autorisé. Ces règles sont à consigner par écrit et à respecter.

6. Il est à noter que d'autres formes d'accès à distance par les membres du personnel des entités surveillées (c'est-à-dire dans le cadre de voyages professionnels, par exemple par des gestionnaires de relation client lors de la participation à des conférences ou à des formations professionnelles), de même que les connexions depuis les locaux de l'employeur à des systèmes non hébergés au sein des locaux de l'employeur ne sont pas inclus dans le champ d'application de la présente circulaire.

7. Afin de lever toute ambiguïté, toute tâche effectuée par les membres du personnel des entités surveillées sur un site autre que les locaux de l'employeur dans le cadre de l'activation d'un plan de rétablissement après sinistre (*Disaster Recovery Plan, DRP*) ou d'un plan de continuité des activités (*Business Continuity Plan, BCP*) n'est pas considérée comme du télétravail et ne relève, par conséquent, pas du champ d'application de la présente circulaire.

Personnel ou membre du personnel

8. Par « personnel » ou « membre du personnel » on entend l'ensemble des employés des entités surveillées, y compris les fonctions clés et la direction autorisée. Les personnes mises à la disposition d'une entité surveillée dans le cadre d'un contrat avec un employeur tiers sont également considérées comme des membres du personnel.

9. Aux fins de la présente circulaire, un membre du personnel qui accomplit ses tâches via le télétravail est un « télétravailleur ».

Locaux de l'employeur ou locaux

10. La notion de « locaux de l'employeur » inclut le siège social et tous les autres locaux au Luxembourg utilisés par les entités surveillées, de même que, dans le contexte de succursales, les locaux des succursales des entités surveillées ou des succursales luxembourgeoises des entités.

Utilisateurs privilégiés

11. Les utilisateurs privilégiés sont les utilisateurs disposant de droits d'accès leur permettant d'effectuer des opérations sensibles, aussi bien dans le cadre d'opérations de TIC (p. ex. les administrateurs de systèmes) que d'opérations relatives à l'activité. Ces opérations sensibles sont généralement liées à l'exécution d'activités critiques.

Activités critiques

12. Par activités critiques on entend les activités pour lesquelles la survenue d'un problème peut avoir des répercussions significatives sur la capacité de l'entité surveillée de respecter les exigences réglementaires ou même de poursuivre ses activités (p. ex. le traitement des transactions, l'insertion ou le téléchargement des ordres, la validation selon le principe des 4 yeux, l'accès administratif à distance aux systèmes des TIC par l'équipe chargée des TIC, etc.).

Direction autorisée

13. Par « direction autorisée » on entend les personnes autorisées par la CSSF chargées de la gestion journalière ou les personnes autorisées par la CSSF qui dirigent de fait les activités d'une entité surveillée.

III. Principes généraux

14. Les entités surveillées doivent maintenir, à tout moment, une administration centrale robuste au Luxembourg et une substance suffisante en leurs locaux, afin de permettre une prise en charge rapide des urgences et autres problèmes dont la résolution est liée au facteur temps. Cependant, les entités surveillées peuvent autoriser leur personnel à exécuter des tâches et activités via le télétravail. En principe, tout membre du personnel, indépendamment de sa fonction, peut être autorisé à télétravailler dans les limites définies dans la présente circulaire dans le but de garantir une gouvernance adéquate de l'entité surveillée et conformément au cadre légal et réglementaire relatif au télétravail en vigueur. La présente circulaire ne créé pas de précédent par rapport à des droits ou obligations relatifs à la possibilité de mettre en œuvre des solutions de télétravail pour les entités soumises à la surveillance de la CSSF. De plus, les relations contractuelles entre les entités surveillées et leurs employés sont exclues du champ d'application de la présente circulaire.

15. Chaque entité surveillée devrait évaluer dans quelle mesure elle autorise son personnel à travailler à distance. Cette évaluation devrait tenir compte des risques liés au télétravail et définir les limites dans lesquelles le personnel pourrait être autorisé à effectuer des tâches à distance. En particulier, les entités surveillées de plus petite taille, employant un nombre restreint de personnes, pourraient se voir obligées d'adapter leur organisation interne, compte tenu des exigences liées à leur taille.

16. Le télétravail ne doit, en aucun cas, compromettre le fonctionnement opérationnel régulier d'une entité surveillée. Il doit être suffisamment robuste pour permettre la continuité effective et sécurisée des activités de l'entité et la continuité opérationnelle de l'ensemble des éléments relevant du cadre du contrôle interne de l'entité, sans exception et de manière continue. L'entité surveillée doit protéger, à tout moment, même dans le cadre du télétravail, la confidentialité, l'intégrité et la disponibilité des données et des systèmes d'informations de l'entité.

17. Le télétravail est organisé sous la responsabilité ultime du conseil d'administration de l'entité surveillée ou de toute autre organe représentant l'entité surveillée en vertu de la loi et des documents constitutifs.

18. La mise en œuvre d'une solution de télétravail ne requiert pas d'autorisation de la CSSF.

IV. Respect d'autres dispositions légales

19. Le recours au télétravail par les entités surveillées ne peut contrevenir aux dispositions légales relevant des règles d'ordre public et doit, en particulier, respecter les dispositions du Code du travail luxembourgeois.

20. De plus, les entités surveillées doivent tenir compte du fait que les exigences prudentielles relatives à la substance et à l'administration centrale peuvent diverger d'autres dispositions légales, en particulier des lois et règlements en matière fiscale (au niveau national, étranger et international), ainsi que des lois et règlements en matière de droit des sociétés ou relatifs au secret professionnel, à la protection des données et à la sécurité sociale. La CSSF s'attend à ce que les entités surveillées tiennent dûment compte de ces lois lors de la mise en œuvre du télétravail, en particulier dans le cadre de l'exécution du télétravail par les membres du personnel non-résidents. La présente circulaire ne doit pas être interprétée par les entités surveillées de manière à contourner les lois et règlements en vigueur.

21. En outre, chaque entité surveillée est tenue de respecter les règlementations européennes et nationales relatives au libre établissement et à la libre prestation de services lors du recours au télétravail.

22. La présente circulaire ne crée pas de précédent par rapport à des droits ou obligations relatifs à la mise en œuvre du télétravail par les entités soumises à la surveillance de la CSSF. Les relations contractuelles entre les entités surveillées et leurs employés sont exclues du champ d'application de la présente circulaire.

V. Exigences de base

23. Une administration centrale robuste est constituée d'un « centre décisionnel » et d'un « centre administratif », ce qui inclut du personnel suffisant en nombre et disposant des qualifications, des connaissances et de l'expertise nécessaires, ainsi que des infrastructures techniques et administratives nécessaires à l'exercice de ses fonctions ou activités.

24. Afin d'être en conformité avec cette exigence d'administration centrale, les membres du personnel doivent être en mesure de se rendre dans de brefs délais dans les locaux de l'entité surveillée en cas de besoin.

25. En ce qui concerne les succursales d'entités surveillées situées en dehors du Luxembourg, il y a lieu de s'assurer que le personnel soit en mesure de se rendre dans de brefs délais dans les locaux de la succursale en cas de besoin.

26. Il relève de la responsabilité du conseil d'administration de l'entité surveillée ou de tout autre organe représentant l'entité surveillée en vertu de la loi et des documents constitutifs, de définir, au préalable, l'étendue du télétravail conformément aux lois et règlements applicables, sans qu'il y ait violation des exigences d'administration centrale.

27. Les critères spécifiques de base suivants sont à respecter lors de la mise en œuvre, l'utilisation ou l'extension du télétravail :

    a. Le nombre de personnes d'une entité surveillée autorisé à télétravailler simultanément doit être en ligne avec les exigences relatives à l'administration centrale.

    b. La durée du temps de travail normal autorisée dans le cadre du télétravail pour chaque membre du personnel devrait être limitée.

    c. En principe, au moins un directeur autorisé doit être présent au siège social de l'entité à tout moment. De plus, les fonctions clés doivent être représentées tous les jours en nombre suffisant dans les locaux de l'entité et garantir, en permanence, le fonctionnement adéquat des activités et des contrôles, ainsi qu'un processus de prise de décision approprié. Pour ce faire, les entités surveillées doivent tenir compte de la taille et de l'organisation de l'entité surveillée et de la nature, de l'échelle et de la complexité de ses activités.

    d. L'entité surveillée doit être en mesure de démontrer que le siège social est à tout moment le « centre décisionnel » faisant partie de l'administration centrale de l'entité surveillée.

    e. La CSSF rappelle en particulier aux entités surveillées que la continuité des activités critiques doit être assurée. Par conséquent, cet aspect est

à prendre en compte de manière adéquate lors de la mise en œuvre du télétravail et de la politique y relative.

i. En ce sens, les entités surveillées doivent s'assurer que les interruptions de télétravail (par exemple les perturbations de connexion) n'entraînent pas de répercussions majeures sur la capacité des entités de poursuivre leurs activités de manière adéquate, rapide et sécurisée.

ii. Les entités surveillées sont tenues de prendre toutes les dispositions visant à assurer que les activités critiques puissent être couvertes par un membre du personnel disposant de qualifications et de responsabilité suffisantes en présentiel dans les locaux de l'entité en vue de garantir le fonctionnement adéquat des activités et des contrôles pendant les heures de travail.

VI. Dispositif d'organisation interne et de contrôle interne

Gestion des risques

28. L'entité surveillée est tenue de procéder à une analyse des risques dans le but d'identifier les risques inhérents à la mise en œuvre du télétravail, en particulier les risques opérationnels, y compris le risque juridique, les risques liés aux technologies de l'information et de la communication (TIC), de *compliance* et de réputation.

29. Une attention particulière devrait être portée :

    a. à l'évaluation des aspects liés au droit du travail et au droit fiscal (y compris les questions relatives à l'établissement permanent), ainsi qu'au droit des sociétés et aux exigences relevant du régime de la sécurité sociale ;

    b. au risque associé au télétravail des utilisateurs privilégiés ;

    c. au respect du secret professionnel et des exigences en matière de protection des données (par exemple, les circonstances dans lesquelles il est permis que les équipements ou documents professionnels sortent de l'environnement professionnel sécurisé).

30. Les entités surveillées sont tenues d'assurer la mise en œuvre des contrôles et des mesures d'atténuation nécessaires en vue de maintenir les risques résiduels dans des limites acceptables en fonction de l'appétit au risque des entités. L'identification des risques et la mise en place des mesures d'atténuation devraient être adéquatement formalisées.

31. Les entités surveillées devraient revoir régulièrement leur analyse des risques et l'adéquation des mesures d'atténuation mises en œuvre, tenant compte des leçons tirées, des changements éventuels dans leur organisation, ou leur environnement, de leurs processus de travail ou leur architecture technique relative au télétravail, ainsi que des nouvelles menaces, telles que la cybercriminalité ou les attaques opportunistes dans un contexte de télétravail.

Politique relative au télétravail

32. Le conseil d'administration de l'entité surveillée ou tout autre organe représentant l'entité surveillée en vertu de la loi et des documents constitutifs est tenu de définir une politique encadrant le télétravail et les limites dans lesquelles le télétravail est autorisé. Cette politique doit clairement définir :

    a. les unités opérationnelles ou les départements pour lesquels le recours au télétravail est possible et les activités et/ou fonctions pouvant être exercées en télétravail ;

    b. les fonctions et/ou activités des unités opérationnelles ou des départements devant toujours être exercées dans les locaux de l'entité surveillée ;

    c. le nombre minimum de personnel devant travailler simultanément dans les locaux au Luxembourg au niveau de l'entité et, le cas échéant, au niveau de l'unité opérationnelle ou du département ;

    d. les heures de travail durant lesquelles le télétravail est autorisé ;

    e. les procédures de contrôle à mettre en œuvre afin d'être en mesure de contrôler la bonne exécution des tâches accomplies par le personnel en télétravail ;

    f. le nombre minimum de réunions présentielles devant se tenir au siège social au Luxembourg ;

    g. les mesures à prendre afin d'assurer que les risques restent maîtrisés, y compris le respect de la règlementation relative à la confidentialité et à la protection des données.

33. La politique doit fixer le cadre opérationnel permettant à la direction autorisée de contrôler le nombre de personnes effectivement en télétravail.

34. Les systèmes d'information d'une entité surveillée et l'environnement de contrôle en vigueur ne peuvent pas être modifiés tant que l'exécution des tâches est autorisée via le télétravail. Les contrôles existants (p. ex. le contrôle selon le principe des 4 yeux), les tableaux de bord (*dashboards*) et le reporting sont à exécuter de la même façon et à la même fréquence, tel que défini dans les procédures internes existantes de l'entité surveillée.

35. Le conseil d'administration de l'entité surveillée ou tout autre organe représentant l'entité surveillée en vertu de la loi et des documents constitutifs est tenu de revoir la politique relative au télétravail tous les ans, en se basant sur l'analyse des risques actualisée et ses objectifs opérationnels et de gestion.

Contrôle du recours au télétravail

36. La CSSF contrôle le respect des obligations découlant de cette circulaire. À cet effet, les entités surveillées sont tenues de conserver les preuves permettant le contrôle du respect des obligations découlant de la politique relative au télétravail (p. ex. l'enregistrement du nom, de la fonction et du département/service pour chaque membre du personnel accomplissant ses tâches via le télétravail). Ces éléments peuvent également permettre de démontrer le respect de ces obligations à des auditeurs indépendants et à la CSSF. L'entité surveillée doit mettre à disposition de la CSSF, à la demande de celle-ci, l'ensemble des preuves justificatives reprises dans la phrase précédente ou les éléments essentiels de celles-ci permettant de démontrer que les présentes obligations ont été respectées, en format électronique exploitable (p.ex. un format de base de données couramment utilisé). L'entité surveillée doit mettre à disposition de la CSSF, à la demande de celle-ci, toutes les informations nécessaires permettant à la CSSF d'effectuer une surveillance effective de l'entité surveillée, y compris, le cas échéant, de la politique relative au télétravail.

Contrôles du télétravail par les fonctions de contrôle interne

37. Les fonctions de contrôle interne, telles que (le cas échéant) les fonctions *compliance*, gestion des risques, y compris la sécurité de l'information (RSSI/CISO) et l'audit interne, sont tenues d'intégrer la révision de la politique relative au télétravail, des flux des processus et du respect des exigences légales et règlementaires dans leur programme de travail pluriannuel respectif, ainsi que, le cas échéant, le compte-rendu de tout problème ou de toute constatation en relation avec le télétravail à la CSSF dans leur rapport de synthèse annuel respectif.

38. De plus, tous les ans, les rapports de synthèse annuels doivent indiquer, s'il y a lieu, tout incident opérationnel significatif en relation avec le télétravail qui aurait pu se produire durant l'année. Ces rapports doivent également inclure de brèves statistiques relatives au recours au télétravail durant l'année.

Commission de Surveillance du Secteur Financier

VII. Exigences en matière de risques liés aux TIC et de risques de sécurité

39. En principe, l'ensemble des paragraphes repris sous la présente section s'appliquent à toutes les entités surveillées. Lors de la mise en œuvre de ces obligations, les entités surveillées devraient tenir compte du principe de proportionnalité en prenant en considération la nature, l'échelle et la complexité de leurs activités. Certains risques pourraient requérir des mesures relatives aux TIC et des mesures de sécurité plus élevées ou en permettre de moins élevées que celles décrites dans cette section. Il relève de la responsabilité des entités surveillées de s'assurer que les conditions relatives aux TIC et les conditions de sécurité sur base desquelles elles autorisent le télétravail de leurs employés soient proportionnelles aux risques auxquels les entités surveillées sont ou pourraient être exposées.

Politiques et procédures

40. Les procédures de sécurité de l'entité surveillée doivent définir les principes et les règles de haut niveau applicables dans le cadre du télétravail afin de protéger la confidentialité, l'intégrité et la disponibilité des données et des systèmes liés aux TIC de l'entité. Ces principes et ces règles peuvent soit faire partie du document de politique de sécurité général ou être inclus dans le document reprenant la politique relative au télétravail et il y est fait référence, pour les deux cas de figure, par les termes « politique de sécurité relative au télétravail ». La politique de sécurité relative au télétravail doit être alignée aux résultats du processus d'évaluation des risques et approuvée par le conseil d'administration de l'entité surveillée ou de toute autre instance représentant l'entité surveillée en vertu de la loi et des documents constitutifs.

41. La politique de sécurité relative au télétravail doit s'accompagner au niveau opérationnel d'une adaptation des procédures d'utilisation existantes ou d'une intégration dans celles-ci, selon le cas. Les politiques, procédures et documents y relatifs concernant le télétravail sont régulièrement à mettre à jour et à communiquer aux membres du personnel.

Sensibilisation aux risques

42. L'entité surveillée est tenue de veiller à ce que tous les membres du personnel soient sensibilisés aux risques et aux meilleures pratiques liés au recours au télétravail (p.ex. par le biais de sessions de formation périodiques, de lettres d'information ou d'autres formes de communication) ainsi qu'aux devoirs et responsabilités qui leur incombent en relation avec les politiques et

procédures de sécurité pertinentes en vue de limiter les erreurs humaines, vols, fraudes, abus ou pertes.

43. Les initiatives et/ou procédures de sensibilisation aux risques et la documentation y relative, reprises ci-avant, doivent couvrir les risques organisationnels et techniques (p.ex. l'ingénierie sociale, les attaques par phishing, etc.) liés au télétravail ainsi que le comportement spécifique à adopter par les télétravailleurs.

Droits d'accès

44. L'entité surveillée est tenue de revoir et adapter ses procédures de gestion des droits d'accès et les accès octroyés dans le cadre du télétravail en fonction de son évaluation des risques et de sa politique de sécurité relative au télétravail.

45. En particulier, les entités surveillées devraient envisager la nécessité de créer des rôles/profils d'utilisateurs et des droits d'accès dédiés aux situations de télétravail (présentant par exemple des limitations par rapport au travail sur site), tout en préservant le principe de la ségrégation des tâches.

46. Les droits d'accès des télétravailleurs (y compris des fournisseurs de service) devraient être octroyés sur base du principe du « besoin d'en connaître » (*need-to-know principle*) et être recertifiés au moins annuellement pour les utilisateurs non-privilégiés et au moins semestriellement pour les utilisateurs privilégiés.

Dispositifs d'accès à distance

47. L'entité surveillée doit s'assurer de garder le contrôle sur la sécurité des dispositifs utilisés par les utilisateurs pour se connecter à distance aux systèmes des TIC de l'entité surveillée. En particulier, l'entité surveillée devrait s'assurer que :

    a. lorsque les données peuvent être enregistrées sur le dispositif, le support de stockage doit être crypté. Le recours à des infrastructures de bureaux virtuels (*Virtual Desktop Infrastructures* ou VDI) qui permettent d'éviter l'enregistrement sur le dispositif, est encouragé ;

    b. les mécanismes de sécurité mis en place par l'entité surveillée ne doivent pas pouvoir être modifiés, supprimés ou contournés par les membres du personnel.

48. Le meilleur moyen pour parvenir au respect des obligations reprises ci-avant est de mettre à disposition des dispositifs appartenant à l'entité, et qui sont entièrement sous le contrôle de l'entité surveillée.

49. La sécurisation des dispositifs privés n'est pas assimilable à celle des dispositifs appartenant à l'entité ; c'est la raison pour laquelle ce genre d'équipement ne devrait être utilisé que pour des activités et systèmes à faible risque. De plus, les membres du personnel effectuant des activités critiques ne doivent pas utiliser des dispositifs privés pour l'accomplissement de telles activités. Les équipes TIC en particulier ne doivent pas être en mesure d'accéder et de gérer des systèmes des TIC au moyen de dispositifs privés.

50. Une éventuelle utilisation de dispositifs privés doit être considérée avec attention et évaluée au moyen d'une analyse des risques spécifique. Malgré le fait que l'entité surveillée ne soit pas propriétaire du dispositif, elle doit être en mesure de contrôler les données et les applicatifs professionnels qui vont y être traités. Des solutions prévoyant que l'entité surveillée installe un environnement professionnel maîtrisé (*container*) à l'intérieur de l'environnement privé de l'outil devrait permettre une maîtrise totale de ce *container*. Des solutions basées sur l'utilisation d'une infrastructure de bureau virtuel (VDI) à partir d'un dispositif privé peuvent être envisagées tant que l'entité surveillée est à même d'atténuer les risques découlant d'un dispositif privé potentiellement compromis. De plus, des tests indépendants doivent être effectués régulièrement afin de prouver que les solutions utilisant des dispositifs privés sont suffisamment sécurisées.

51. Enfin, l'entité surveillée doit s'assurer que les dispositifs appartenant à l'entité ou, le cas échéant, le *container* professionnel du dispositif privé puissent être gérés à distance par une solution de gestion centralisée.

Infrastructure de télétravail

52. L'entité surveillée est tenue de maintenir un niveau élevé de sécurité et de disponibilité de l'infrastructure de télétravail dans le temps. Dans ce contexte, l'entité surveillée veille à ce que, à tout moment, les diverses composantes fonctionnent correctement, qu'elles soient adéquatement sécurisées et contrôlées de près.

53. L'entité surveillée doit mettre en œuvre des mécanismes lui permettant de détecter des connexions anormales et de les bloquer/générer des alertes y relatives.

54. En particulier, aux fins du point 53, l'entité surveillée doit définir un ensemble de critères et obligations tant relatifs à la sécurité que non relatifs à la sécurité devant être assurés avant de permettre à un télétravailleur d'accéder aux systèmes et données internes, sur base des risques identifiés lors de la

réalisation de l'évaluation des risques. Dans ce contexte, une liste non-exhaustive de critères et obligations possibles est reprise ci-après :

a. le télétravailleur est correctement authentifié ;

b. le dispositif est correctement identifié et authentifié ;

c. la localisation à distance du télétravailleur est correctement identifiée ;

d. le temps de connexion se situe endéans les plages horaires de travail définies ;

e. les composants et mécanismes de sécurité mis en œuvre par l'entité surveillée n'ont pas été modifiés ou contournés par le télétravailleur ou par un pirate informatique, et sont à jour et opérationnels.

55. Afin de pouvoir maintenir l'infrastructure de télétravail dans le temps, l'entité surveillée aura mis en place un processus de gestion du changement robuste, permettant d'assurer que l'infrastructure de télétravail mise en œuvre et le niveau de sécurité ne seront pas compromis en cas de changements.

Sécurité des connexions

56. L'entité surveillée doit s'assurer que le transfert des données est sécurisé, c'est-à-dire chiffré, conformément à la classification des données par l'entité et que les protocoles de chiffrement mis en place (p.ex. IPSec, SSL), les algorithmes de chiffrement (p.ex. RSA, AES) ainsi que la taille de la clé de chiffrement choisie respectent les pratiques actuelles de référence.

57. Une authentification à double facteur (2-FA) doit être mise en place lors d'une connexion à distance aux systèmes de l'entité surveillée.

58. Le mécanisme d'authentification mis en place peut être adapté en fonction du type d'opérations effectuées à distance et du profil de l'utilisateur (principe de proportionnalité).

59. En ce qui concerne les activités critiques, les entités surveillées sont censées mettre en place une procédure d'authentification forte à double facteur, dont l'un des facteurs doit être dynamique (p.ex. un OTP).

Revue de la sécurité de la chaîne de communication

60. Le fonctionnement correct de la chaîne de communication entre le dispositif à distance et l'infrastructure de la société (par exemple la passerelle d'accès à distance, ou *remote access gateway*) ainsi que l'efficacité des mesures de sécurité mises en place doivent être revus par une fonction de contrôle de la sécurité indépendante (c.-à-d. le responsable de la sécurité des systèmes d'informations, l'audit interne ou un tiers externe spécialisé) avant la mise en place du télétravail et, par la suite, sur une base régulière.

61. Cette revue doit en particulier confirmer que l'infrastructure mise en place, le positionnement des différentes barrières de sécurité et les mécanismes de sécurité et de prévention de fuites de données appliqués sont correctement conçus, testés, implémentés et configurés.

62. De plus, l'entité surveillée devrait procéder régulièrement à des analyses de vulnérabilité et à des tests d'intrusion, proportionnellement au niveau de risque identifié en relation avec le télétravail.

Veille technologique

63. Un solide processus de veille technologique devrait être en place permettant à l'entité surveillée d'être rapidement informée de l'apparition de nouvelles failles de sécurité et d'y appliquer les correctifs nécessaires dans de brefs délais. Une attention particulière est à apporter aux risques liés à l'utilisation de dispositifs privés lorsque leur utilisation est permise.

Processus de journalisation (logging)

64. Un processus de journalisation (*logging*) sain est à mettre en place, afin de permettre aux entités surveillées de s'assurer que toutes les connexions et informations techniques pertinentes relatives au télétravail (y compris le dispositif de connexion utilisé) soient enregistrées à des fins de contrôle de sécurité.

65. Les *logs* d'accès doivent être sécurisés afin d'en empêcher toute modification ou effacement non autorisé. Le principe de proportionnalité doit être assuré, par exemple la granularité de l'information enregistrée et la période de conservation de l'enregistrement doivent être proportionnels à la criticité de l'opération exécutée par le télétravailleur, sans préjudice des exigences de conservation des données définies par le droit de l'Union et la règlementation nationale.

VIII. Entrée en vigueur, révision et disposition anti-abus

66. La présente circulaire entre en vigueur le 30 septembre 2021, sauf circonstances exceptionnelles telles que définies à la page 2.

67. Sur base de l'expérience tirée du contrôle auquel il est fait référence au point 36, la présente circulaire sera revue au plus tard 12 mois après son entrée en vigueur, afin de remédier à d'éventuels abus ou autres lacunes ou défaillances.

Commission de Surveillance du Secteur Financier

Claude WAMPACH
Directeur

Marco ZWICK
Directeur

Jean-Pierre FABER
Directeur

Françoise KAUTHEN
Directeur

Claude MARX
Directeur Général

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