Commission de Surveillance du Secteur Financier

Luxembourg, le 17 mai 2017

A tous les établissements de monnaie électronique, établissements de paiement et PSF autres que les entreprises d'investissement[1]

# CIRCULAIRE CSSF 17/656

**Concerne: Organisation administrative et comptable; sous-traitance en matière informatique**

Mesdames, Messieurs,

La présente circulaire a pour objet de préciser les modalités d'application de l'article 17(2) de la loi du 5 avril 1993 telle que modifiée (la LSF) pour les professionnels du secteur financier (ci-après désignés par PSF) et des articles 11(2) et (4) et 24-7 (2) et (4) de la loi du 10 novembre 2009 relative aux services de paiement (la LSP) pour les établissements de monnaie électronique et établissements de paiement, lorsqu'ils ont recours à un tiers en matière informatique.

Ce faisant, elle aligne les obligations applicables à tous les établissements de monnaie électronique, établissements de paiement et PSF autres que les entreprises d'investissement, au contenu de la circulaire CSSF 12/552 applicable aux établissements de crédits et entreprises d'investissement. Elle apporte également des précisions sur les conditions de sous-traitance informatique applicables spécifiquement aux PSF de support et leurs éventuelles succursales situées à l'étranger.

La présente circulaire abroge et remplace la circulaire CSSF 05/178.

Le chapitre 1 de la présente circulaire s'aligne sur la forme et le fond au sous-chapitre 7.4 « Sous-traitance » (outsourcing) de la circulaire CSSF 12/552, applicable aux établissements de crédits et entreprises d'investissement. Pour faciliter la gestion parallèle d'éventuelles évolutions futures, il est choisi de faire correspondre la numérotation des paragraphes de ce chapitre 1 à celle des paragraphes du sous-chapitre 7.4 de la circulaire CSSF 12/552, d'où une numérotation commençant par 181. La sous-section 2.1 et les points 198, 199 et 201 de la sous-section 2.3 du chapitre 1 ne sont pas applicables aux PSF visés par les articles 29-3, 29-4, 29-5 et 29-6 et dénommés « PSF de support ».

Le chapitre 2 précise les conditions à respecter par un PSF de support et ses éventuelles succursales situées à l'étranger, pour recourir à une sous-traitance informatique autre que celle répondant à la circulaire CSSF 17/654 portant sur le « cloud computing ». Il est à noter que les PSF de support permettent d'apporter un cadre juridique certain, réglementé et surveillé au phénomène de sous-traitance, appelée également *outsourcing*, d'activités du secteur financier. L'article 41(5) de la loi précise que l'obligation au secret n'existe pas à l'égard des PSF de support dans la mesure où les renseignements communiqués à ces professionnels sont fournis dans le cadre d'un contrat de services

[1] La circulaire CSSF 05/178 ne s'applique plus aux établissements de crédit et aux entreprises d'investissement. Pour ces entités, la circulaire a été remplacée par la circulaire CSSF 12/552, telle que modifiée.

relevant de l'une des activités réglementées et à condition que ces renseignements soient indispensables à l'exécution du contrat de services en cause.

Ce second chapitre est sans lien avec la circulaire CSSF 12/552 ; c'est pourquoi la numérotation de ses paragraphes est totalement déconnectée de celle utilisée au chapitre précédent.

## Chapitre 1. Sous-traitance

181. La sous-traitance désigne le transfert complet ou partiel de tâches opérationnelles, d'activités ou de prestations de services de l'établissement vers un prestataire externe, qui fait partie ou non du groupe auquel l'établissement appartient.

Lorsqu'une sous-traitance de nature informatique, ou une chaîne de sous-traitance composée exclusivement de sous-traitances de nature informatique, repose sur une infrastructure de cloud computing telle que définie dans la circulaire 17/654, les points de la présente circulaire ne s'appliquent pas et il convient au professionnel financier de respecter les exigences de la circulaire 17/654.

Pour les besoins de cette circulaire, le terme « activité » sert à désigner les tâches opérationnelles, activités et prestations de services visées au premier paragraphe. Est considérée comme « matérielle » toute activité qui, lorsqu'elle n'est pas exécutée dans les règles, diminue la capacité de l'établissement à respecter les exigences réglementaires ou à poursuivre ses opérations, ainsi que toute activité qui est nécessaire à la gestion saine et prudente des risques.

### Section 1. Exigences générales en matière de sous-traitance

182. La sous-traitance ne doit pas aboutir à ce que les règles en matière d'administration centrale ne soient plus respectées.

L'établissement qui sous-traite se conforme en particulier aux exigences suivantes :

- Les fonctions stratégiques ou relevant du cœur de métier ne peuvent pas être sous-traitées ;
- L'établissement conserve l'expertise nécessaire pour contrôler efficacement les prestations ou les tâches sous-traitées et la gestion des risques associés à la sous-traitance ;
- La protection des données doit être garantie en permanence ;
- La sous-traitance ne décharge pas l'établissement de ses obligations légales et réglementaires ou de ses responsabilités envers la clientèle. Elle n'entraîne aucune délégation de responsabilité de l'établissement vers le sous-traitant, sauf concernant la responsabilité du secret professionnel lorsque le sous-traitant agit dans le cadre de l'article 41(5) de la LSF ;
- La responsabilité finale de la gestion des risques associés à la sous-traitance incombe à la direction autorisée de l'établissement procédant à la sous-traitance ;
- L'établissement s'assure, au regard des éventuels risques juridiques et obligations légales, de la nécessité d'informer ou non, respectivement d'obtenir le consentement, des tiers concernés par cette sous-traitance et notamment des clients du secteur financier. A ce titre, l'établissement respecte la réglementation applicable au regard de la protection des données personnelles.
- La confidentialité et l'intégrité des données et des systèmes doivent être maîtrisées dans toute la chaîne de sous-traitance. Notamment, l'accès aux données et systèmes doit respecter les principes du « besoin de savoir » et du « moindre privilège » : l'accès n'est octroyé qu'aux personnes dont la fonction le justifie, dans un but précis, et leurs privilèges sont restreints au strict minimum nécessaire pour exercer leurs fonctions ;

- L'établissement qui a l'intention de sous-traiter une activité matérielle doit obtenir l'autorisation préalable de la CSSF. Une notification à la CSSF, justifiant que les conditions fixées dans la présente circulaire sont respectées, est suffisante lorsque l'établissement recourt à un établissement de crédit luxembourgeois ou à un PSF de support selon les articles 29-1 à 29-6 de la LSF ;
- L'accès de la CSSF, du réviseur d'entreprises agréé et des fonctions de contrôle interne de l'établissement aux informations relatives aux activités sous-traitées doit être garanti en vue de leur permettre d'émettre une opinion fondée sur l'adéquation de la sous-traitance. Cet accès inclut que les précités peuvent également vérifier les données pertinentes détenues par un partenaire externe et, dans les cas prévues par la législation nationale, ont le pouvoir de mener des contrôles sur place chez un partenaire externe. L'opinion précitée peut, le cas échéant, se baser sur les rapports du réviseur externe du sous-traitant.

183. L'établissement qui sous-traite appuie sa décision de sous-traiter sur une analyse préalable et approfondie, démontrant qu'elle n'entraîne pas de délocalisation de l'administration centrale. Celle-ci portera au moins sur une description circonstanciée des services ou activités à sous-traiter, sur les effets attendus de la sous-traitance ainsi que sur une évaluation approfondie des risques du projet de sous-traitance envisagé sur le plan des risques financiers, opérationnels, légaux et de réputation.

184. Une attention particulière doit être portée à la sous-traitance d'activités critiques au niveau desquelles la survenance d'un problème pourrait avoir un effet significatif sur la capacité de l'établissement à respecter les exigences réglementaires, voire à poursuivre son activité.

185. Une attention particulière doit être accordée aux risques de concentration et de dépendance qui apparaissent lorsque de larges parties d'activités ou de fonctions importantes sont sous-traitées à un prestataire unique pendant une période prolongée.

186. Les établissements doivent prendre en compte les risques associés aux «chaînes» de sous-traitance (lorsqu'un prestataire sous-traite une partie des activités sous-traitées à d'autres prestataires). A cet égard ils accordent une attention particulière à la sauvegarde de l'intégrité du contrôle interne et externe. En outre, l'établissement veillera à fournir à la CSSF tous les éléments permettant de montrer que le processus de sous-traitance en cascade est maîtrisé.

187. La politique en matière de sous-traitance tient compte de l'impact de la sous-traitance sur les activités et les risques de l'établissement. Elle fixe les exigences de *reporting* auxquelles sont soumis les prestataires et le dispositif de contrôle que l'établissement met en place à leur égard pour la durée intégrale de la sous-traitance. La sous-traitance ne peut en aucun cas avoir pour effet de contourner des restrictions réglementaires ou des mesures prudentielles de la CSSF ou d'entraver la surveillance par la CSSF.

188. Une attention particulière doit être accordée aux aspects de continuité et au caractère révocable de la sous-traitance. L'établissement doit être capable de maintenir ses fonctions critiques en cas d'évènements exceptionnels ou de crises. A ce titre, les contrats de sous-traitance ne contiennent pas de clause de résiliation ou d'arrêt des prestations en raison de l'application à l'établissement de mesures d'assainissement ou d'une procédure de liquidation ou, le cas échéant, une procédure de faillite, de gestion contrôlée, de sursis de paiement, de concordat préventif de faillite ou autres procédures analogues.[2] L'établissement prendra également les précautions qui s'imposent afin d'être à même de transférer de manière adéquate les services sous-traités à un autre fournisseur ou de les reprendre en gestion propre, chaque fois que la continuité ou la qualité de la prestation de service risque d'être compromise.

[2] Cette disposition diverge de la disposition équivalente présente au point 188 de la circulaire CSSF 12/552 car elle est adaptée aux types d'entités concernées.

189. Pour chaque activité sous-traitée, l'établissement désignera parmi ses employés une personne qui aura la responsabilité de la gestion de la relation de sous-traitance ainsi que la charge de gérer l'accès aux données confidentielles.

## Section 2. Exigences particulières en matière de sous-traitance dans le domaine informatique

190. L'établissement met en place une politique informatique qui couvre l'ensemble des activités informatiques réparties entre l'établissement et tous les intervenants de la chaîne de sous-traitance. L'organisation informatique est adaptée de manière à intégrer les activités sous-traitées au bon fonctionnement de l'établissement et le manuel de procédures est adapté en conséquence. Le plan de continuité de l'établissement est établi en cohérence avec le plan de continuité de son ou ses sous-traitants.

191. La politique de l'établissement en matière de sécurité des systèmes d'information prend en compte la sécurité individuelle mise en place par son ou ses sous-traitants, afin de s'assurer notamment de la cohérence de l'ensemble.

192. La sous-traitance en matière informatique peut porter sur des services de conseil, de développement et de maintenance (sous-section 2.2), des services d'hébergement (sous-section 2.3) ou des services de gestion/d'opération des systèmes informatiques (sous-section 2.1).

### Sous-section 2.1. Services de gestion/d'opération des systèmes informatiques

193. Les établissements peuvent recourir contractuellement à des services de gestion/d'opération de leurs systèmes :

- Au Luxembourg, uniquement auprès :
  - d'un établissement de crédit ou d'un professionnel financier disposant d'un agrément de PSF de support selon les articles 29-3 et 29-4 de la LSF (statut d'opérateurs de systèmes informatiques primaires du secteur financier, également appelés « OSIP », ou statut d'opérateurs de systèmes informatiques secondaires et de réseaux de communication du secteur financier, également appelés « OSIS ») ;
  - d'une entité du groupe auquel l'établissement appartient et qui traite exclusivement des opérations de groupe, à condition que ces systèmes ne contiennent aucune donnée confidentielle lisible concernant les clients. Dans le cas contraire, l'établissement s'assure, au regard des éventuels risques juridiques et obligations légales, de la nécessité d'informer ou non, respectivement d'obtenir le consentement, des tiers concernés par cette sous-traitance et notamment des clients du secteur financier. A ce titre, l'établissement respecte la réglementation applicable au regard de la protection des données personnelles.
- A l'étranger, auprès :
  - de tout prestataire informatique, y compris auprès d'une entité du groupe auquel l'établissement appartient, à condition que ces systèmes ne contiennent aucune donnée confidentielle lisible concernant les clients. Dans le cas contraire, l'établissement s'assure, au regard des éventuels risques juridiques et obligations légales, de la nécessité d'informer ou non, respectivement d'obtenir le consentement, des tiers concernés par cette sous-traitance et notamment des clients du secteur financier. A ce titre, l'établissement respecte la réglementation applicable au regard de la protection des données personnelles.

### Sous-section 2.2. Services de conseil, de développement et de maintenance

194. Les services de conseil, de développement et de maintenance peuvent être contractés avec tout prestataire informatique, y compris un service informatique du groupe auquel l'établissement appartient ou un PSF de support.

195. Des tiers sous-traitants autres que les PSF de support qui fournissent des services de conseil, de développement ou de maintenance doivent intervenir par défaut hors du système informatique de production. Si une situation exceptionnelle rend nécessaire une intervention sur le système de production et que l'accès à des données confidentielles ne peut pas être évité, l'établissement doit veiller à ce que le tiers en question soit surveillé tout au long de sa mission par une personne de l'établissement en charge de l'informatique. Un accord exprès de l'établissement est nécessaire pour chacune des interventions sur le système de production, à l'exception des interventions réalisées par un PSF de support dans le cadre de son mandat.

196. Toute modification des fonctionnalités des applications par un tiers - autres que des modifications liées à de la maintenance corrective – doit être soumise pour accord à l'établissement, préalablement à sa mise en production.

197. L'établissement s'assurera qu'en cas de nécessité, il n'y ait aucun obstacle juridique pour avoir accès aux programmes d'exploitation qui ont été développés par un tiers sous-traitant. Ce but peut être atteint notamment lorsque l'établissement est juridiquement propriétaire des programmes. L'établissement s'assurera de la possibilité de poursuivre l'exploitation des applications critiques à l'activité en cas de défaillance du sous-traitant, pour une période compatible avec un transfert de cette sous-traitance vers un autre sous-traitant ou une reprise en mains propres des applications concernées.

**Sous-section 2.3. Services d'hébergement et propriété de l'infrastructure**

198. L'infrastructure informatique peut appartenir à l'établissement ou être mise à disposition par le sous-traitant.

Lorsque l'infrastructure informatique contient des données confidentielles, seul le personnel du PSF de support ou l'établissement de crédit luxembourgeois peut indifféremment travailler dans ses locaux ou ceux du professionnel financier sans encadrement particulier de la part du personnel de l'établissement, à condition que la prestation relève de l'article 41(5) de la LSF et fasse l'objet d'un contrat de service permettant cette autonomie. Lorsque le sous-traitant n'est pas PSF de support ou établissement de crédit luxembourgeois, l'établissement s'assure, au regard des éventuels risques juridiques et obligations légales, de la nécessité d'informer ou non, respectivement d'obtenir le consentement, des tiers concernés par cette sous-traitance et notamment des clients du secteur financier. A défaut, le sous-traitant ne peut intervenir sur l'infrastructure de l'établissement sans être accompagné tout au long de sa mission par une personne de l'établissement en charge de l'informatique.

Lorsque l'infrastructure informatique ne contient pas de données confidentielles, un accord exprès de l'établissement est nécessaire pour chacune des interventions sur l'infrastructure informatique par un tiers, à l'exception des interventions réalisées par un PSF de support dans le cadre de son mandat.

199. Il n'est pas exigé que le centre de traitement soit physiquement localisé auprès de l'entité contractuellement responsable de la gestion des systèmes informatiques. Que le centre de traitement soit au Luxembourg ou à l'étranger, il est donc possible que l'hébergement du site soit confié à un autre prestataire que celui qui preste les services de gestion des systèmes informatiques. Dans ce cas l'établissement doit s'assurer que les principes énoncés dans le présent sous-chapitre sont respectés par l'entité contractuellement responsable de la gestion des systèmes informatiques et que le processus de sous-traitance en cascade est maîtrisé.

200. Lorsque le centre de traitement est au Luxembourg, il peut être logé auprès d'un prestataire autre qu'un établissement de crédit ou un PSF de support, à condition que celui-ci n'ait aucun accès physique et logique sur les systèmes de l'établissement.

201. Lorsque le centre de traitement est à l'étranger, aucune donnée confidentielle de nature à identifier un client de l'établissement ne peut y être stockée sans être protégée. La confidentialité et l'intégrité des données et des systèmes doivent être maîtrisées dans toute la chaîne de sous-traitance. Notamment, l'accès aux données et systèmes doit respecter les principes du « besoin de

savoir » et du « moindre privilège » : l'accès n'est octroyé qu'aux personnes dont la fonction le justifie, dans un but précis, et leurs privilèges sont restreints au strict minimum nécessaire pour exercer leurs fonctions. L'établissement s'assure, au regard des éventuels risques juridiques et obligations légales, de la nécessité d'informer ou non, respectivement d'obtenir le consentement, des tiers concernés par cette sous-traitance et notamment des clients du secteur financier.

### Section 3. Exigences générales supplémentaires

202. Afin de permettre à l'établissement d'apprécier la fiabilité et l'exhaustivité des données produites par le système informatique ainsi que leur compatibilité avec les prescriptions comptables et de contrôle interne, il doit avoir parmi ses employés une personne ayant les connaissances nécessaires en matière informatique pour comprendre à la fois les effets que les programmes produisent sur le système comptable et les actions réalisées par le tiers dans le cadre des services rendus.

    L'établissement doit également disposer dans ses locaux d'une documentation suffisante des programmes utilisés

203. En cas de prestation de services informatiques par voie de télécommunication, l'établissement doit s'assurer :

    - que des mesures de protection suffisantes sont prises afin d'éviter que des personnes non autorisées ne puissent accéder à son système. L'établissement doit prévoir notamment que les télécommunications soient cryptées ou encore protégées selon d'autres moyens techniques disponibles de nature à assurer la sécurité des communications ;
    - que la liaison informatique permet à l'établissement luxembourgeois d'avoir un accès rapide et non limité aux informations stockées dans l'unité de traitement (par exemple grâce à un chemin d'accès et un débit adaptés et grâce à des solutions de redondance).

204. L'établissement doit s'assurer que les mécanismes de saisie, d'impression, de sauvegarde, de stockage et d'archivage garantissent la confidentialité des données.

205. La sous-traitance ne doit pas aboutir à transférer la fonction financière et comptable à un tiers. L'établissement disposera à la fin de chaque jour d'une balance de tous les comptes et de tous les mouvements comptables de la journée. Le système doit permettre de tenir une comptabilité régulière suivant les normes en vigueur au Luxembourg et donc de respecter les règles de forme et de fond imposées par la réglementation comptable luxembourgeoise.

206. Lorsque l'établissement opère à l'étranger en recourant aux services d'intermédiaires professionnels (même s'ils font partie du groupe auquel l'établissement appartient) ou lorsqu'il y dispose de succursales ou de bureaux de représentation, tout accès par ces intermédiaires ou les représentants et employés de ces bureaux et succursales à son système d'informations au Luxembourg doit faire l'objet d'une autorisation par la CSSF.

### Section 4. Documentation

207. Toute sous-traitance d'activités matérielles ou non, y compris celle qui est réalisée au sein du groupe auquel l'établissement appartient, s'inscrit dans une politique écrite et nécessitant une approbation de la direction autorisée, incluant des plans d'urgence et des stratégies de sortie. Tout accord de sous-traitance fait l'objet d'un contrat officiel et détaillé (cahier des charges inclus).

208. La documentation écrite fournit également une description claire des responsabilités des deux parties ainsi que les moyens de communication clairs, assortis d'une obligation pour le prestataire de services externe de signaler tout problème important ayant un impact sur les activités sous-traitées, ainsi que toute situation d'urgence.

209. Les établissements prennent les dispositions nécessaires pour assurer que les fonctions de contrôle interne ont accès à tout moment et sans encombre à toute documentation relative aux activités sous-traitées et que ces fonctions gardent la pleine possibilité d'exercer leurs contrôles.

## Chapitre 2. Le recours à une sous-traitance informatique autre que celle répondant à la circulaire CSSF 17/654 portant sur le « cloud computing » par un PSF de support et ses éventuelles succursales situées à l'étranger

A. Les PSF de support et leurs succursales agissant en qualité d'OSIP ou d'OSIS peuvent recourir, pour leurs prestations d'opérateurs de systèmes, à des infrastructures appartenant à leur groupe, à condition que les services prestés par le groupe ou leurs éventuels sous-traitants, soient limités à ceux nécessitant une présence physique sur ces infrastructures et à l'exclusion de toute gestion des systèmes contenant les données et traitements à charge du PSF de support. Par infrastructure, il faut comprendre les ressources informatiques nécessaires à l'hébergement des systèmes et des données dont l'opérateur de systèmes OSIP ou OSIS a la gestion.

   Dans ce cas, les PSF de support doivent particulièrement veiller à garder un contrôle permanent sur les actions réalisées par le groupe pour leur compte. Lorsque cette sous-traitance implique la présence sur l'infrastructure concernée, d'informations relevant du secret professionnel de leurs clients professionnels financiers, et particulièrement s'il s'agit d'informations relatives aux clients finaux de ces professionnels financiers, les PSF de support seront tenus d'obtenir l'accord des professionnels financiers concernés avant de procéder à la sous-traitance envisagée.

B. Les PSF de support et leurs succursales peuvent choisir de sous-traiter une partie ou la totalité de l'informatique à usage interne à un prestataire tiers. Par informatique à usage interne, il faut comprendre l'informatique qui exclut celle proposée comme service à des tiers ou celle utilisée par des services proposés à des tiers[3]. Les PSF de support concernés devront notifier préalablement leur choix à la CSSF, y compris lorsqu'ils concernent leurs succursales, en confirmant en quoi ils respectent les éléments de la présente circulaire. Lorsque la sous-traitance adresse des informations relevant du secret professionnel de leurs clients professionnels financiers, notamment les informations relatives aux clients finaux de ces professionnels financiers, les PSF de support seront tenus d'obtenir l'accord des professionnels financiers concernés avant de procéder à la sous-traitance envisagée.

C. Les succursales des PSF de support peuvent proposer à leurs clients du pays d'accueil où elles sont établies, des services reposant sur une infrastructure établie dans le pays d'accueil. Cette infrastructure peut être sous-traitée à un prestataire local à condition que les services prestés par ce prestataire et ses éventuels sous-traitants, soient limités à ceux nécessitant une présence physique sur ces infrastructures et à l'exclusion de toute gestion des systèmes contenant les données et traitements à charge du PSF de support ou de sa succursale. La succursale applique alors les principes énoncés dans la présente circulaire et le siège au Luxembourg conserve le contrôle adéquat des prestations réalisées par sa succursale. Les succursales devront obtenir des professionnels financiers concernés l'accord pour cette sous-traitance locale.

D. Sauf cas particulier nécessitant une autorisation spécifique de la CSSF sur base d'arguments dûment justifiés, les succursales des PSF de support ne peuvent pas fournir leurs services d'opérations de systèmes au siège, sauf pour les services à usage interne. Une telle situation amènerait une succursale à prester les services d'opérations de systèmes aux clients du siège en vidant le PSF de support de sa substance.

[3] A titre d'exemple, il s'agit de la messagerie d'entreprise, de stockage de documents, de comptabilité interne, de téléphonie VoIP, de CRM, etc.

**Entrée en vigueur et dispositions diverses**

La présente circulaire entre en vigueur avec effet immédiat ; elle abroge et remplace la circulaire CSSF 05/178.

Veuillez recevoir, Mesdames, Messieurs, l'assurance de nos sentiments très distingués.

COMMISSION de SURVEILLANCE du SECTEUR FINANCIER



| Jean-Pierre FABER | Françoise KAUTHEN | Claude SIMON |
|---|---|---|
| Directeur | Directeur | Directeur |


| Simone DELCOURT | Claude MARX |
|---|---|
| Directeur | Directeur général |