Luxembourg, le 11 avril 2005

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

# CIRCULAIRE CSSF 05/178

**Concerne: Organisation administrative et comptable; sous-traitance en matière informatique; abrogation du point 4.5.2. de la circulaire IML 96/126 et remplacement par le point 4.5.2. de la présente circulaire.**

Mesdames, Messieurs,

La présente circulaire a pour objet de préciser les modalités d'application de l'article 5(2) de la loi du 5 avril 1993 relative au secteur financier (ci-après désignée par « la loi ») pour les banques et de l'article 17(2) de la loi pour les professionnels du secteur financier (ci-après désignés par PSF) lorsqu'un professionnel financier a recours à un tiers en matière informatique. La circulaire modifie certaines dispositions prévues par la circulaire IML 96/126, notamment en ce qui concerne le recours à une sous-traitance à l'étranger auprès d'une entité surveillée du groupe ou lorsque le professionnel financier fait appel à un PSF qui exerce une activité connexe ou complémentaire à une activité du secteur financier.

[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.

Ces nouvelles catégories de PSF, définies aux articles 29-1, 29-2 et 29-3 de la loi et reprises ci-après sous la dénomination de « PSF connexes », permettent en effet d'apporter un cadre juridique certain, réglementé et surveillé au phénomène de sous-traitance, appelée également *outsourcing*, d'activités du secteur financier. Il est à noter que l'article 41(5) de la loi précise que l'obligation au secret n'existe pas à l'égard des professionnels visés aux articles 29-1, 29-2 et 29-3, dans la mesure où les renseignements communiqués à ces professionnels sont fournis dans le cadre d'un contrat de services relevant de l'une des activités réglementées et à condition que ces renseignements soient indispensables à l'exécution du contrat de services en cause. A noter que les catégories de PSF définies aux articles 29-1 et 29-2 de la loi, qui répondent également à la définition de PSF connexe en raison de l'activité complémentaire, ne relèvent pas en premier chef de la sous-traitance informatique et sont dès lors exclues de l'application de la présente circulaire.

Si la sous-traitance peut, dans de bonnes conditions, contribuer à une meilleure gestion par le transfert de certaines fonctions à des tiers disposant d'une plus grande expertise et permettant des économies d'échelle accrues, elle ne diminue en rien la responsabilité des professionnels financiers de tenir compte des principes de saine gestion dans toutes les activités. Il appartient dès lors aux professionnels financiers de mener une politique appropriée en matière de sous-traitance d'activités, en particulier en vue du maintien d'une organisation adéquate.

L'organisation adéquate des professionnels financiers, ainsi que le contrôle de cette organisation, constituent en effet les pierres angulaires du contrôle prudentiel.

La sous-traitance d'activités ne peut porter préjudice au contrôle interne du professionnel financier et à la qualité du contrôle externe, ni à la protection des clients.

En conformité avec les recommandations en matière d'*outsourcing* discutées au niveau international, les professionnels financiers qui ont recours à une sous-traitance doivent respecter les conditions suivantes :

a) La sous-traitance doit être inscrite dans une politique de sous-traitance documentée et validée par le conseil d'administration. Le professionnel financier appuie sa décision de sous-traiter sur une analyse approfondie. 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. Le

professionnel financier documentera dûment ce processus, en vue du contrôle interne et externe.

b) Toute sous-traitance doit être formalisée par un contrat de services avec un cahier des charges qui tient compte des conditions énumérées ci-dessous. Une attention particulière sera accordée à cet égard aux aspects de continuité, au caractère révocable de la sous-traitance et au maintien de l'intégrité du contrôle interne et externe. En outre, la convention fournira une description claire des responsabilités des deux parties. Le professionnel financier passera des accords clairs avec le fournisseur de services externes en ce qui concerne les conditions auxquelles existe éventuellement le droit de sous-traiter à nouveau à des tiers tout ou partie de l'activité sous-traitée (sous-traitance en cascade).

c) Le professionnel financier s'assurera, au regard des éventuels risques juridiques ou autres, de la nécessité d'informer ou non les tiers concernés par cette sous-traitance et notamment les clients. Les risques à considérer pourraient découler, à titre d'exemple, d'une incompatibilité de la sous-traitance avec certaines clauses contractuelles vis-à-vis de ces tiers ou avec certaines dispositions légales, nationales ou étrangères, en matière de protection de la vie privée.

d) Pour chaque activité sous-traitée, le professionnel financier désignera parmi ses employés une personne qui aura la responsabilité de la gestion de la relation de sous-traitance.

e) Le professionnel financier doit être en mesure de continuer à fonctionner normalement en cas d'événements exceptionnels, tels que la rupture des moyens de communication avec le centre de traitement ou le dysfonctionnement de celui-ci, ceci pendant des périodes prolongées.

f) Le professionnel financier 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.

En ce qui concerne la fonction informatique en tant que fonction de support, le point 4.5.2 de la circulaire IML 96/126 est remplacé par le point 4.5.2 de la présente circulaire.

Quatre cas de figure sont notamment considérés ci-après au sein du texte du point 4.5.2., à savoir :

- Le recours à une sous-traitance informatique pour des prestations ne relevant pas des services de gestion et d'opérations des systèmes informatiques et des réseaux de communication,
- Le recours à une sous-traitance informatique au sein du groupe,
- Le recours à une sous-traitance informatique au sein du groupe, mais à l'étranger,
- Le recours à une sous-traitance informatique auprès d'un PSF connexe au Luxembourg.

4.5.2. La fonction informatique

Les professionnels financiers doivent organiser leur fonction informatique de manière à en avoir le contrôle et à en assurer la qualité et de manière à garantir strictement la protection des données confidentielles qui leur sont confiées par leurs clients.

4.5.2.1. - Ces exigences sont le mieux remplies lorsque la fonction informatique du professionnel financier est prise en charge par son propre service informatique organisé et encadré par un dispositif de contrôle interne fixé par la direction. En règle générale, le professionnel financier disposera, dans des locaux à sa disposition au Luxembourg, de ses propres ordinateurs et de programmes informatiques appropriés et dûment documentés et engagera un personnel compétent pour gérer son système informatique. Par ailleurs, le professionnel financier doit être en mesure de fonctionner normalement en cas de panne de son système informatique et il élaborera à cet effet une solution de « back-up » en adéquation avec un plan de continuité des activités. Le plan de continuité vise à décrire les actions à mettre en œuvre afin de poursuivre les activités en cas d'incident ou sinistre lié à des événements anormaux.

- Il est admissible que les professionnels financiers disposant de leur propre ordinateur recourent aux services d'un tiers en matière de conseil, de programmation ou de maintenance de leurs systèmes. Par contre, les services de gestion des systèmes relèvent du statut d'opérateurs de systèmes informatiques et de réseaux de communication du secteur financier (art.29-3 de la loi). Les professionnels financiers ne peuvent par conséquent recourir à des services de gestion de leurs systèmes qu'auprès de professionnels financiers disposant d'un agrément selon l'article 29-3 de la loi ou, à condition que ces systèmes ne contiennent aucune donnée confidentielle lisible, auprès d'une entité surveillée du groupe (Cf. 4.5.2.2) ou auprès

d’une entité du groupe bénéficiant de l’exception de l’article 13(2). Le tiers fournissant des services de conseil, de programmation ou de maintenance de systèmes peut être notamment une société spécialisée en informatique appartenant ou non au professionnel financier, une société spécialisée en informatique créée conjointement avec d'autres professionnels financiers (banques ou PSF) qui coopèrent en matière informatique ou encore un PSF connexe. Les professionnels financiers concernés ne peuvent cependant pas se soustraire à la responsabilité qu'ils assument pour garder secrets les renseignements qui leur ont été confiés, sauf à l’égard d’un PSF connexe, dans le cadre du contrat de service relevant des missions confiées.

En cas de recours à de tels services auprès de prestataires autres que les PSF connexes, les professionnels financiers s'exposent à un risque de divulgation plus important que dans l'hypothèse où ils utilisent leur propre personnel pour gérer leur système informatique.

Etant donné ce risque, il importe que les professionnels financiers ayant recours aux services de tiers respectent les conditions suivantes:

a) Tout recours aux services d'un tiers doit être formalisé par un contrat de services avec un cahier des charges qui tient compte des conditions énumérées ci-dessous.

b) Le recours aux services informatiques d'un tiers ne doit pas aboutir à transférer la fonction comptable, y compris la saisie des données, auprès de ce tiers.

c) Afin de permettre au professionnel financier 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:

   - Prévoir que toute intervention d'un tiers autre qu’un PSF connexe, notamment toute modification apportée aux programmes soit soumise à son accord préalable.

   - 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.

° Disposer dans ses locaux d'une documentation suffisante des programmes utilisés.

d) Le professionnel financier 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 ce tiers. Ce but peut être atteint notamment lorsque le professionnel financier est juridiquement propriétaire des programmes. Le professionnel financier anticipera les actions à entreprendre pour garantir la pérennité des services prestés en cas de défaillance du tiers.

e) Pour des raisons de protection et de confidentialité les tiers en question autres que les PSF connexes ne peuvent pas avoir accès à des données confidentielles.

f) L'interdiction d'accéder à des données confidentielles vaut également pour des tiers autres que les PSF connexes qui sont en charge de la maintenance du système informatique et éventuellement de sa gestion dans le cas d'une entité du groupe. Si, dans le cadre d'une panne importante du système qui rend nécessaire un dépannage sur place, l'accès à ces données ne peut pas être évité, le professionnel financier doit veiller que le tiers en charge du dépannage soit accompagné tout au long de sa mission par une personne du professionnel financier en charge de l'informatique.

g) Chaque professionnel financier désignera parmi ses employés une personne qui aura la charge de gérer l'accès aux données confidentielles.

h) Quelle que soit la nature de l'intervention sur les programmes (conseil, gestion, maintenance ou modification), les tiers en question ne peuvent travailler que dans un environnement test et nécessitent l'accord exprès du professionnel financier pour chaque intervention, à l'exception des interventions réalisées par un PSF connexe dans le cadre de son mandat.

i) En cas de prestation de services informatiques par voie de télécommunication, le professionnel financier doit s'assurer que des mesures de protection suffisantes soient prises afin d'éviter que des personnes non autorisées ne puissent accéder à son système. Le professionnel financier doit prévoir notamment que les télécommunications soient encryptées ou encore protégées selon d'autres moyens techniques disponibles de nature à assurer la sécurité des communications.

Le professionnel financier doit s'assurer par ailleurs que des mesures soient prévues pour lui permettre de continuer de fonctionner normalement lorsqu'il y a une rupture de la ligne ou un dysfonctionnement de celle-ci pendant des périodes prolongées.

4.5.2.2. Lorsque les conditions précises et restrictives définies ci-après sont respectées il peut être considéré que les obligations en matière d'organisation de la fonction informatique sont également respectées par un professionnel financier qui fait gérer ses données par un centre de traitement informatique qui ne lui appartient pas ou dont il n'est que copropriétaire et auquel il est lié par voie de télécommunication.

Lorsque le centre de traitement est à l'étranger, la sous-traitance doit contractuellement être confiée à la maison-mère (ou, en cas de succursales, auprès du siège) ou une filiale de celle-ci ou encore auprès d'une société spécialisée en traitement informatique contrôlée par le groupe auquel le professionnel financier appartient. L'entité responsable de la prestation doit tomber dans le champ d'application du contrôle prudentiel exercé par une autorité de contrôle prudentiel étrangère. Il n'est pas exigé que le centre de traitement soit physiquement localisé auprès de l'entité responsable. Lorsque le centre de traitement est physiquement localisé auprès de ou opéré par une entité juridique autre que celle à laquelle le traitement a été contractuellement confié, le professionnel financier devra s'assurer que les principes énoncés au point 4.5.2.1 soient respectés par l'entité surveillée, contractuellement responsable. Le professionnel financier veillera à fournir à la CSSF tous les éléments permettant de montrer que le processus de sous-traitance en cascade est maîtrisé. A cette fin, il présentera un document qui indique que les autres autorités de surveillance concernées ont connaissance de cette sous-traitance, en précisant si possible le périmètre de leur surveillance dans ce contexte.

Aucune donnée confidentielle de nature à identifier un client du professionnel financier ne peut être stockée auprès d'un centre de traitement autre qu'un PSF connexe, à moins d'être cryptée et à condition que le décryptage ne puisse se faire qu'au sein du professionnel financier ou d'un PSF connexe dans le cadre de sa prestation.

Lorsque le centre de traitement est au Luxembourg, il peut être logé dans une société du groupe qui traite exclusivement des opérations du groupe, conformément

à l'article 13(2) de la loi, mais dans ce cas il ne doit contenir aucune donnée lisible susceptible de permettre une identification de client. Par ailleurs, il est admissible que le centre de traitement soit logé dans une société qui est détenue et contrôlée conjointement par plusieurs professionnels financiers luxembourgeois (banques ou PSF) qui coopèrent en matière informatique. Dans ce cas, le centre commun traite exclusivement des opérations pour compte de ces professionnels financiers, mais doit disposer d'un agrément de PSF connexe.

Les professionnels financiers qui envisagent de faire traiter leurs données par un centre de traitement informatique à l'étranger auprès d'une entité soumise à la surveillance prudentielle ne peuvent cependant pas se soustraire à la responsabilité qu'ils assument pour garder secrets les renseignements confiés à eux dans le cadre de leur activité professionnelle. En cas de recours à une telle solution, les professionnels financiers s'exposent à un risque de divulgation plus important que lorsqu'ils utilisent une des solutions reprises au point 4.5.2.1. ou lorsqu'ils font appel aux services d'un PSF connexe.

Un professionnel financier qui envisage de recourir à une de ces organisations autres qu'un PSF connexe demandera l'accord préalable de la CSSF en prouvant que les conditions fixées dans la présente circulaire sont respectées.

Les professionnels financiers qui veulent mettre en place une telle structure, indifféremment du fait que le prestataire soit PSF connexe ou non, doivent respecter au moins les conditions suivantes en complément à celles reprises au point 4.5.2.1. :

a) La liaison informatique doit permettre au professionnel financier luxembourgeois d'avoir un accès rapide et non limité aux informations stockées dans l'unité de traitement. La saisie des données s'effectuera intégralement dans les locaux au Luxembourg par l'usage de terminaux et l'impression des données s'effectuera exclusivement dans les locaux du professionnel financier au Luxembourg ou dans ceux d'un PSF connexe.

   Par exception, des données peuvent être saisies ou imprimées en dehors des locaux du professionnel financier par un client ou un mandataire initiant des opérations au moyen d'une liaison télématique.

Le professionnel financier disposera à la fin de chaque jour d'une balance de tous les comptes et de tous les mouvements comptables de la journée.

b) 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.

c) Les communications entre le professionnel financier et le centre de traitement doivent être encryptées ou encore être protégées selon d'autres moyens techniques disponibles de nature à assurer la sécurité des communications. Aucun nom de client ne sera saisi ou inscrit dans le système auquel des tiers, autre qu'un PSF connexe, auront accès.

d) Le réviseur d'entreprises du professionnel financier et le service d'audit interne du professionnel financier devront être en mesure d'effectuer dans le centre de traitement les contrôles nécessaires pour pouvoir émettre une opinion fondée sur l'adéquation de la liaison informatique.

e) La liaison informatique doit être formalisée par un contrat de services et un cahier des charges qui tiennent compte des conditions énumérées ci-dessus.

Les professionnels financiers qui actuellement font traiter leurs données au moyen d'une telle liaison et qui ne respectent pas les conditions définies ci-dessus sont priés de se mettre en rapport avec la CSSF pour lui présenter les mesures qu'ils envisagent de prendre afin de disposer d'une fonction informatique répondant aux conditions de la présente circulaire.

4.5.2.3. Lorsque le professionnel financier opère à l'étranger en recourant aux services d'intermédiaires professionnels (même s'ils font partie du groupe auquel le professionnel financier appartient) ou lorsqu'il y dispose de bureaux de représentation, ces intermédiaires ou les représentants de ces bureaux ne peuvent en aucun cas avoir accès à son système informatique au Luxembourg.

4.5.2.4 Les exigences de contrôle, de qualité et de garantie stricte de la protection des données confidentielles à respecter par les professionnels financiers, sont remplies lorsque le professionnel financier a recours à un PSF connexe. Dans ce cas, l'organisation sera adaptée de manière à intégrer les activités sous-traitées au bon fonctionnement du professionnel financier et le manuel de procédures sera adapté en conséquence. Le plan de continuité du professionnel financier sera établi en cohérence avec le plan de continuité du PSF connexe.

L'infrastructure informatique peut appartenir au professionnel financier ou être mis à disposition par le PSF connexe. Le personnel du PSF connexe peut indifféremment travailler dans ses locaux ou ceux du professionnel financier.

A noter les précisions suivantes :

a) L'obligation au secret n'existe pas à l'égard des professionnels visés à l'article 29-3 de la loi, dans la mesure où les renseignements communiqués à ces professionnels sont fournis dans le cadre d'un contrat de services relevant de l'activité réglementée par la disposition légale susmentionnée et à condition que ces renseignements soient indispensables à l'exécution du contrat de services en cause. (article 41(5))

b) Le réviseur d'entreprise du professionnel financier et le service d'audit interne du professionnel financier doivent être en mesure d'effectuer auprès du PSF connexe les contrôles nécessaires pour pouvoir émettre une opinion fondée sur l'adéquation de la liaison informatique. Le cas échéant, ils peuvent se baser sur les rapports du réviseur externe du PSF connexe.

c) Un professionnel financier qui recourt à un PSF connexe le notifiera à la CSSF en justifiant que les conditions fixées dans la présente circulaire sont respectées.

La CSSF estime souhaitable que les conventions de sous-traitance existantes soient, dans la mesure du possible, adaptées aux principes de la présente circulaire avant le 31 décembre 2005. Elle demande aux professionnels concernés de tendre vers cet objectif et attend en tout cas que cette adaptation se fasse lors de la prochaine modification ou prolongation de toute convention existante.

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

COMMISSION DE SURVEILLANCE DU SECTEUR FINANCIER

| Simone DELCOURT | Arthur PHILIPPE | Jean-Nicolas SCHAUS |
|---|---|---|
| Directeur | Directeur | Directeur général |