Commission de Surveillance du Secteur Financier

Luxembourg, le 17 mai 2017

A tous les établissements de crédit, entreprises d'investissement et professionnels effectuant des opérations de prêt

CIRCULAIRE CSSF 17/655

Concerne : Mise à jour de la circulaire CSSF 12/552 relative à l'administration centrale, la gouvernance interne et la gestion des risques

Mesdames, Messieurs,

1. La présente circulaire a pour objet de modifier la circulaire CSSF 12/552 relative à l'administration centrale, la gouvernance interne et la gestion des risques. La circulaire CSSF 12/552 est modifiée comme suit :

- Dans la note de bas de page n° 3 à la page 2, la première phrase « Les circulaires IML 95/120, IML 96/126, IML 98/143 et CSSF 05/178 restent en vigueur pour les PSF qui ne sont pas des entreprises d'investissement. » est remplacée par « Les circulaires IML 95/120, IML 96/126, IML 98/143 restent en vigueur pour les PSF qui ne sont pas des entreprises d'investissement ainsi que la circulaire CSSF 17/656 qui abroge et remplace la circulaire CSSF 05/178. »

- Au 6ème tiret du point 17, après « les principes directeurs en matière de sous-traitance (« outsourcing ») », les mots suivants sont insérés : « y compris de nature informatique se reposant ou non sur une infrastructure de « cloud computing » ».

- Au point 85, il est inséré le nouveau paragraphe suivant après le troisième paragraphe :

  « L'établissement se dote d'un processus de veille lui permettant d'être informé rapidement de l'apparition de nouvelles failles de sécurité d'une part, et d'une procédure de gestion des patchs devant permettre dans un délai réduit la correction desdites failles, dès lors qu'elles peuvent impacter significativement son système informatique. L'audit interne intègre dans son plan d'audit pluriannuel la revue du processus de veille et de la gestion des patchs ; il relève notamment tout manquement dans la mise en production d'un patch alors que celui-ci est notablement connu et documente les raisons d'un tel manquement dans un point d'audit. »

- Au point 181, il est inséré le nouveau paragraphe suivant après le premier paragraphe :

« 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 du sous-chapitre 7.4 de la présente circulaire ne s'appliquent pas et il convient au professionnel financier de respecter les exigences de la circulaire 17/654. »

- Au point 182, le deuxième paragraphe est modifié comme suit :
  - Le 6ème tiret :

  « L'établissement s'assure, 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 ; »

  est remplacé par :

  « 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. »

  - Le 7ème tiret :

  « La confidentialité des données doit être garantie en permanence, sauf consentement explicite du client ou du propriétaire des données ou de son représentant, donné sur base d'un avis éclairé concernant l'intérêt de cette sous-traitance, la spécificité de la finalité recherchée, du contenu de l'information transmise, du destinataire et de la localisation, ainsi que de la durée dans le temps ; »

  est remplacé par :

  « 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 ; »

  - A la fin du 8ème tiret, la référence aux articles de la LSF est étendue comme suit : « selon les articles 29-1 à 29-6 de la LSF ».

- Au point 188 :

- La deuxième phrase :

« L'établissement doit être en mesure de continuer à fonctionner normalement en cas d'événements exceptionnels ou de crise. »

est remplacée par :

« L'établissement doit être capable de maintenir ses fonctions critiques en cas d'évènements exceptionnels ou de crises. »

- La troisième phrase :

« 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 telles que prévues à la partie IV de la LSF. »

est remplacée par :

« 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 de résolution ou d'assainissement ou d'une procédure de liquidation telles que prévues dans la loi du 18 décembre 2015 relative à la défaillance des établissements de crédit et de certaines entreprises d'investissement. »

- Au point 190, dans la première phrase, « et son ou ses sous-traitants » est remplacé par « et tous les intervenants de la chaîne de sous-traitance. »

- Au point 193 :

  - Sous le tiret « Au Luxembourg, uniquement auprès : », le 2ème sous-tiret :

« 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 autres que des clients institutionnels, sauf s'il existe un consentement explicite du client ou du propriétaire des données ou de son représentant, donné sur base d'un avis éclairé concernant l'intérêt de cette sous-traitance, la spécificité de la finalité recherchée, du contenu de l'information transmise, du destinataire et de la localisation, ainsi que de la durée dans le temps ; concernant les clients institutionnels, les spécificités de cette sous-traitance doivent être explicites dans le contrat. »

est remplacé par :

« 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. »

  - Sous le tiret « A l'étranger, auprès : », le sous-tiret :

« d'une entité du groupe auquel l'établissement appartient, à condition que ces systèmes ne contiennent aucune donnée confidentielle lisible concernant les clients autres que des clients institutionnels, sauf s'il existe un consentement explicite du

client ou du propriétaire des données ou de son représentant, donné sur base d'un avis éclairé concernant l'intérêt de cette sous-traitance, la spécificité de la finalité recherchée, du contenu de l'information transmise, du destinataire et de la localisation, ainsi que de la durée dans le temps ; concernant les clients institutionnels, les spécificités de cette sous-traitance doivent être explicites dans le contrat. »

est remplacé par :

« 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. »

- Au point 195, les deux premières phrases :

  « L'interdiction d'accéder à des données confidentielles vaut pour des tiers sous-traitants autres que les PSF de support qui fournissent des services de conseil, de développement ou de maintenance. Ces tiers doivent intervenir par défaut hors du système informatique de production. »

  sont remplacées par :

  « 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. »

- Au point 198, au deuxième paragraphe :

  - A la première phrase, après « seul le personnel du PSF de support », il est inséré « ou de l'établissement de crédit luxembourgeois ».
  - La dernière phrase :

  « Lorsque le sous-traitant n'est pas PSF de support, il 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. »

  est remplacée par :

  « 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. »

- Le point 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, à moins d'être cryptée et à condition que le décryptage ne puisse se faire qu'au sein de

l'établissement ou d'un PSF de support dans le cadre de sa prestation ou si l'ensemble des clients de l'établissement remplissent les conditions de consentement explicite et éclairé telles que définies au point 193. »

est remplacé par :

« 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. »

Entrée en vigueur et dispositions diverses

2. Les modifications apportées par la présente circulaire à la circulaire CSSF 12/552 entrent en vigueur avec effet immédiat.

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

COMMISSION de SURVEILLANCE du SECTEUR FINANCIER

Jean-Pierre FABER
Directeur

Françoise KAUTHEN
Directeur

Claude SIMON
Directeur

Simone DELCOURT
Directeur

Claude MARX
Directeur général