Repealed by Circular CSSF 17/656

COMMISSION de SURVEILLANCE
du SECTEUR FINANCIER

In case of discrepancies between the French and the English text, the French text shall prevail

Luxembourg, 11 April 2005

To all electronic money institutions, payment institutions as well as PFS other than investment firms[1]

CIRCULAR CSSF 05/178

Re: Administrative and accounting organisation; outsourcing of IT services; abrogation of point 4.5.2. of circular IML 96/126 and replacement by point 4.5.2. of current circular

Ladies and Gentlemen,

The purpose of this circular is to provide details on the implementation of article 5(2) of the law of 5 April 1993 on the financial sector as amended ("the Law") for banks and of article 17(2) for professionals of the financial sector (PFS) where a financial professional relies on a third party for the provision of IT services. This circular amends some provisions set down in circular IML 96/126, in particular in relation to the outsourcing of activities abroad to a supervised entity of the group, or where a financial professional relies on a support PFS.

These new PFS categories, defined under articles 29-1, 29-2 and 29-3 of the Law and hereafter referred to as "support PFS", allow creating a definite legal, as well as regulated and

[1] Circular CSSF 05/178 no longer applies to credit institutions and investment firms. For these entities, the circular has been replaced by Circular CSSF 12/552, as amended.

supervised framework governing the outsourcing of activities of the financial sector. One should note that article 41(5) of the Law stipulates that the obligation to secrecy does not exist towards professionals referred to in articles 29-1, 29-2 and 29-3 insofar as the information communicated to those professionals is provided in pursuance of a service agreement falling within one of the regulated activities and provided that this information is essential to the execution of the service agreement concerned. It should be noted that the PFS categories defined under articles 29-1 and 29-2 of the Law, which correspond as well to the definition of support PFS due to the complementary activity, do not directly fall under the IT outsourcing activity and are thus excluded from the scope of application of this circular.

If outsourcing may, under good conditions, contribute to a better management through the transfer of certain functions to third parties having a greater expertise and allowing accrued scale savings, it does not reduce in any way the responsibility of the financial professionals to take into account the principles of sound management in all activities. Financial professionals should hence adopt an appropriate policy for outsourcing activities, in particular with a view to maintaining an adequate organisation.

The adequate organisation of the financial professionals and the control of this organisation are indeed the cornerstones of prudential supervision.

The outsourcing of activities shall not impair the internal control of financial professionals nor the quality of the external control, nor client protection.

In accordance with the recommendations in relation to outsourcing discussed at international level, financial professionals relying on outsourcing shall meet with the following conditions:

(a) The outsourcing must be in line with a documented outsourcing policy, validated by the board of directors. The financial professional shall base its decision to outsource on an in-depth analysis. This analysis must include at least a detailed description of the services or activities to outsource, the expected results of the outsourcing and an in-depth evaluation of the risks of the outsourcing project as regards financial, operational, legal and reputational risks. The financial professional shall duly document this process, in view of an internal and external control.

(b) Any outsourcing shall be formalised by a service level agreement with requirement specifications taking into account the conditions below. Particular attention must be paid in this respect to aspects such as continuity, the revocability of outsourcing and the

upholding of the internal and external control integrity. Moreover, the agreement shall provide a clear description of the responsibilities of both parties. The financial professional shall make clear agreements with the external service provider on the conditions of a possible further outsourcing to third parties of all or part of the outsourced activity (sub-outsourcing).

(c) The financial professional shall assess, in view of possible legal or other risks, the necessity to inform or not the third parties concerned by this outsourcing, in particular clients. The risks to consider may originate, for example, from an incompatibility of the outsourcing with certain contractual clauses towards those third parties or with certain legal provisions, national or foreign, as regards privacy protection.

(d) For each outsourced activity, the financial professional shall designate among its employees one person that will be responsible for the management of the outsourcing relation.

(e) The financial professional shall be in a position to pursue its operations normally in case of exceptional events, such as interruption of communication means with the processing centre or its dysfunction, during an extended period of time.

(f) The financial professional shall take the necessary measures to be in a position to adequately transfer the outsourced activities to a different provider or to perform those activities itself whenever the continuity or the quality of the service provision are likely to be affected.

In relation to the IT function as a support function, point 4.5.2. of circular IML 96/126 is replaced by point 4.5.2. of current circular.

Four scenarios are considered hereafter within the text of point 4.5.2., namely:

- IT outsourcing for service provisions which do not fall under the management and operation of IT and communication network systems.
- IT outsourcing within the group.
- IT outsourcing within the group, but abroad.
- IT outsourcing with a support PFS in Luxembourg.

4.5.2. The IT function

Financial professionals shall organise their IT function in order to control it, to ensure its quality and to guarantee the strict protection of confidential data entrusted to them by their clients.

4.5.2.1. - These requirements are best fulfilled when the IT function of the financial professional is performed by its own, well organised, IT department supervised by an internal control framework established by the board. Generally, the financial professional must have, in premises at its disposal in Luxembourg, its own computers and adequate and duly documented IT programmes and hire competent personnel to manage its IT system. Moreover, the financial professional shall be in a position to ensure normal operations in case of an IT-system outage and shall put in place a backup solution in line with a business continuity plan. The business continuity plan aims at describing the actions to put in place in order to continue the activities in case of an incident or disaster linked to unusual events.

- Financial professionals with their own computer system may rely on third party for the provision of advisory, programming and system maintenance services. System operation and management services, however, fall under the status of IT systems and communication networks operator of the financial sector (art. 29-3 of the Law). Financial professionals may thus only rely on financial professionals authorised in accordance with article 29-3 of the Law for the provision of IT managed services or, provided that these systems do not include any readable confidential data, on a supervised entity of the group (cf. 4.5.2.2) or on an entity of the group benefiting from the exception provided under article 13(2). A third party providing advisory, programming or system maintenance services may be a specialised company in IT owned or not by the financial professional, a company specialised in IT created jointly with other financial professionals (banks or PFS), which cooperate in IT matters, or also a support PFS. The financial professionals concerned may however not evade their liability to maintain secret the information which is entrusted to them,

except towards a support PFS, in the relation of the service level agreement falling under the tasks entrusted.

Financial professionals are exposed to a higher disclosure risk when resorting to providers other than support PFS for such services than if they were using their own staff to manage their IT system.

Considering this risk, it is important for financial professionals relying on third parties to comply with the following conditions:

(a) Any outsourcing shall be formalised by a service level agreement including the requirement specifications taking into account the conditions below.

(b) Outsourcing IT services shall not result in transferring the accounting function, including data inputing, to this third party.

(c) In order to allow financial professionals to evaluate whether the data produced by the IT system is reliable, comprehensive, and in line with the accounting and internal control principles, it shall:

- Ensure that any intervention of a third party other than a support PFS, in particular any modification brought to the programmes, is subjected to a prior consent.
- Have among its staff a person with the necessary IT knowledge to understand both the effects of the programmes on the accounting system and the actions undertaken by the third party in the context of the service provided.
- Have in its premises sufficient documentation on the programmes used.

(d) The financial professional shall ensure that there are, if needed, no legal obstacles to obtain the access to operating systems which have been developed by this third party. This is achieved, for example, when the financial professional is the legal owner of the programmes. The financial professional shall anticipate the actions to take in order to ensure the continuity of the services provision in case the third party defaults.

(e) For protection and confidentiality reasons, third parties other than support PFS cannot be granted access to confidential data.

(f) The prohibition to access confidential data also applies to third parties other than support PFS in charge of the IT system maintenance and management in the case of an entity owned by the group. If access to some data cannot be avoided when fixing a major system disruption on-site, the financial professional shall ensure that the third party in charge of this intervention is accompanied during the whole mission by an IT-staff member of the financial professional.

(g) Any financial professional shall designate one staff member who will be in charge of managing the access to confidential data.

(h) Whatever intervention is required on the programmes (advice, management, maintenance or modification), the third parties concerned may only work in a test environment and need the explicit agreement of the financial professional for each intervention, except if realised by a support PFS in the context of its mandate.

(i) For remote IT managed services, the financial professional shall ensure that sufficient protection measures are taken in order to avoid that unauthorised persons access its system. The financial professional shall ensure that telecommunications are encrypted or protected through other technical means available to ensure the security of communications.

The financial professional shall moreover ensure that measures are taken to allow normal functioning when lines are interrupted or dysrupted during an extended period of time.

4.5.2.2. The requirements on the IT function organisation are also considered as fulfilled by a financial professional whose datacenter is managed by an IT processing centre not belonging to it or of which it is only a co-owner and to which it is linked through telecommunication whenever the precise and restrictive conditions hereafter defined are met.

When the processing centre is located abroad, the outsourcing shall contractually be entrusted to the parent undertaking (or, in the case of branches, to the head office) or to a subsidiary of the parent undertaking or to a company specialised in IT processing controlled by the group to which the financial professional belongs. The

entity responsible for the service provision must fall under the scope of the prudential supervision performed by a foreign supervisory authority. It is not mandatory for the processing centre to be physically located on the premises of the responsible entity. Where the processing centre is physically located on the premises of or operated by a legal entity other than the one to which the processing has been entrusted with contractually, the financial professional shall ensure that the supervised entity, contractually responsible, complies with the principles indicated under point 4.5.2.1 The financial professional shall ensure to provide the CSSF with any elements allowing to prove that the sub-outsourcing process is under control. To this end, it shall present a document indicating the awareness of the other relevant supervisory authorities of this outsourcing, specifying whenever possible, the extent of their supervision in this context.

No confidential data allowing to identify a client of the financial professional must be stored within a processing centre other than a support PFS, unless it is encrypted and provided the decryption process can only be executed at the premises of the financial professional or of the support PFS in the context of its service provision.

When a datacentre is based in Luxembourg, it may be located within a company of the group which handles exclusively the group's operations, in accordance with article 13(2) of the Law, but in this case, it shall not contain any readable data that might allow the identification of the client. The datacentre may as well be located in a company that is jointly held and controlled by several Luxembourg financial professionals (banks or PFS) that cooperate in IT matters. In this case, the common centre exclusively processes operations on behalf of the financial professionals and must be licensed as a support PFS.

The financial professionals that consider having their data processed by an IT datacentre located abroad within a company subject to prudential supervision remain nevertheless responsible to maintain secrecy on the information entrusted to them in the context of their professional activity. Financial professionals are, in this context, subject to a greater disclosure risk than if using solutions specified under point 4.5.2.1 or appointing a support PFS.

A financial professional considering to rely on one of these organisations, other than a support PFS, shall seek the prior consent of the CSSF by proving that the conditions set out in this circular are satisfied.

Financial professionals intending to set up this type of structure, whether the service provider is a support PFS or not, shall comply with at least the following conditions in addition to those indicated under point 4.5.2.1:

(a) The IT link shall allow the Luxembourg financial professional to have a quick and unlimited access to information stored in the processing unit. Data input will be made entirely in the premises in Luxembourg through terminals. Data printing will be executed exclusively at the premises of the financial professional in Luxembourg or at a support PFS.

Nevertheless, data may be inputed or printed outside the premises of the financial professional by a client or a proxy initiating transactions through a telematic link.

The financial professional is required to have at the closing of each day the balance of all accounts and of all accounting movements of the day.

(b) The system shall allow to hold a regular accounting pursuant to the rules applicable in Luxembourg and thus respect the form and content ruled by the Luxembourg accounting principles.

(c) Communication between the financial professional and the datacentre shall be encrypted or protected by other technical means available to ensure the security of communication. No client name shall be inputed or registered in the system to which third parties, other than support PFS, have access.

(d) The external auditor and the internal audit department of the financial professional shall be in a position to assess the necessary controls in the datacentre in order to issue a well-founded opinion on the adequacy of the IT link.

(e) The IT link shall be set out in a service level agreement with requirement specifications which take into account the above conditions.

The financial professionals which currently have their data processed by means of such a link and which do not satisfy the above conditions are requested to contact the

CSSF to present the measures it contemplates to take for the IT function to comply with the conditions set out in this circular.

4.5.2.3. Where the financial professional operates abroad relying on the services of professional intermediaries (even though they are part of the group to which the financial professional belongs) or where its representative offices are located abroad, the intermediaries or representatives of these offices cannot, in any case, have access to its IT system in Luxembourg.

4.5.2.4 The requirements of control, quality and strict guarantee of confidential data protection imposed on financial professionals are fulfilled when the financial professional relies on a support PFS. In this case, the organisation shall be adapted in order to integrate the outsourced activities to the proper functioning of the financial professional and the procedures manual shall be adapted accordingly. The business continuity plan of the financial professional shall be established in accordance with the contingency plan of the support PFS.

The IT infrastructure may be owned by the financial professional or be provided by the support PFS. The staff of the support PFS may either work at its premises or at the premises of the financial professional.

The following specifications should be considered:

(a) The obligation to secrecy does not exist towards professionals referred to in article 29-3 of the Law insofar as the information communicated to those professionals is provided in pursuance of a service level agreement falling within one of the activities regulated by the above-mentioned legal provisions, and provided that the information concerned is essential to the execution of the services provision in question. (article 41(5))

(b) The external auditor and the internal audit department of the financial professional shall be in a position to carry out the necessary controls on the premises of the support PFS to issue a well-founded opinion on the adequacy

of the IT link. They may refer to the report of the external auditor of the support PFS, where applicable.

(c) A financial professional relying on a support PFS shall notify the CSSF by proving that the conditions laid down in this circular are satisfied.

The CSSF considers that the existing outsourcing conventions should, as far as possible, be adapted to the principles set out in this circular before 31 December 2005. It requires the professionals concerned to move towards this objective and expects at least this adaptation to be included in the next modification or extension of any existing convention.

Yours faithfully,

COMMISSION DE SURVEILLANCE DU SECTEUR FINANCIER

Simone DELCOURT	Arthur PHILIPPE	Jean-Nicolas SCHAUS
Director	Director	Director General