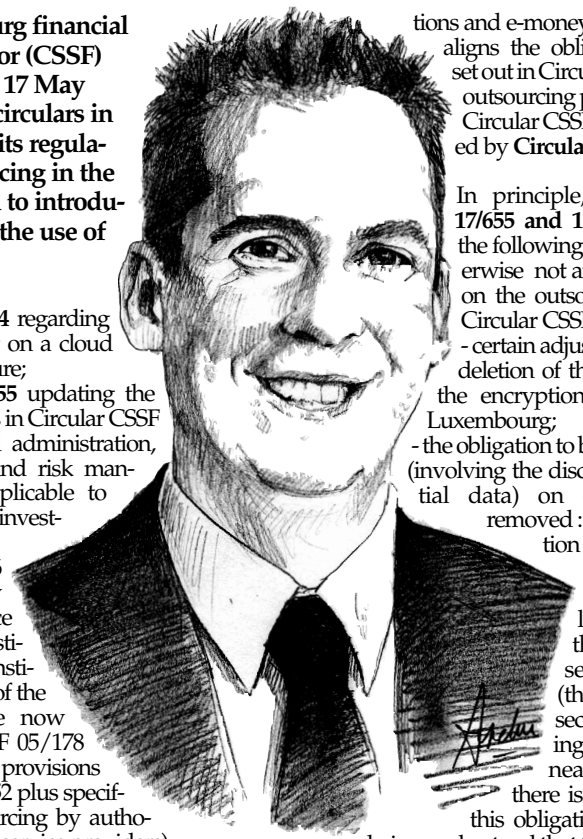
First assessment

The new regulatory framework in the financial sector for outsourcing in Luxembourg and the introduction of specific rules for cloud services

The Luxembourg financial sector regulator (CSSF) published on 17 May 2017 the following circulars in order to streamline its regulation on (IT) outsourcing in the financial sector, and to introduce specific rules for the use of cloud services:



- Circular CSSF 17/654 regarding IT outsourcing relying on a cloud computing infrastructure;
- Circular CSSF 17/655 updating the outsourcing provisions in Circular CSSF 12/552 on the central administration, internal governance and risk management that are applicable to credit institutions and investment firms;
- Circular CSSF 17/656 on the outsourcing by other financial service providers, payment institutions and e-money institutions (i.e. alignment of the rules set out in the now repealed Circular CSSF 05/178 with the outsourcing provisions of Circular CSSF 12/552 plus specific rules on the outsourcing by authorised support financial service providers);
- Circular CSSF 17/657 updating Circular CSSF 06/240 on administrative and accounting organisation (i.e. the adoption of the concept of «operation of IT systems» in order to exclude cloud-based services); amendment of IT outsourcing conditions for branches located abroad.

Through these circulars, the CSSF defines the conditions under which financial service providers may outsource activities, IT-related activities in particular without infringing the regulatory principles of central administration and sound governance. These circulars complement the imminent legislative changes which will foresee in an explicit legal exemption from the professional secrecy obligation in the financial sector as far as outsourcing is concerned.

1. Outsourcing in general

Under Luxembourg law, the regulatory principles of central administration and internal governance in the financial sector are laid down in a very high-level fashion in the Financial Sector Act 1993.

In Circular CSSF 12/552 on the central administration, internal governance and risk management applicable to credit institutions and investment firms, and Circular CSSF 05/178 (repealed and replaced by Circular CSSF 17/656 now) on the administrative and accounting organisation (outsourcing of IT services) of other financial institutions (including payment service providers and e-money institutions), the CSSF has defined a more detailed framework with respect to outsourcing, targeting IT outsourcing in particular. Both circulars contain several similar key elements, such as the need for the outsourcing to be consistent with a predefined policy based on a risk assessment, the need to formalise the outsourcing in an agreement including service levels and specifications and the need for the outsourcing financial institution to control all stages of the outsourcing process.

Both circulars contain important restrictions to outsourcing activities outside Luxembourg to the extent that these involve the processing of confidential data. For operations that involve a potential disclosure of confidential data, the outsourcing should namely be carried out by a so-called IT systems operator of the financial sector within the meaning of Articles 29-3 and 29-4 of the Financial Sector Act 1993, which are entities (often belonging to major IT groups) that need a prior authorisation in this respect and are under the supervision of the CSSF.

Circular CSSF 05/178 was particularly restrictive on the cross-border outsourcing, limiting such operations to some types of intra-group outsourcing. Circular CSSF 12/552 is more liberal in this respect and allows intra- and extra-group outsourcing to some extent, notably when confidential data is encrypted and the decryption can only take place in Luxembourg. Furthermore, Circular CSSF 12/552 allows outsourcing operations involving a potential disclosure of confidential data if the clients of the financial institution consent thereto.

Circular CSSF 17/655 updated Circular CSSF 12/552 (applicable to credit institutions, investment firms as far as the outsourcing provisions are concerned).

Circular CSSF 17/656 repealed and replaced Circular CSSF 05/178 on outsourcing for other financial service providers than credit institutions and investment firms, as well as payment institutions and e-money institutions. It also aligns the obligations previously set out in Circular 05/178 with the outsourcing provisions set out in Circular CSSF 12/552 as amended by **Circular CSSF 17/655**.

In principle, **Circulars CSSF 17/655 and 17/656** shall operate the following changes to the otherwise not amended provisions on the outsourcing set forth in Circular CSSF 12/552:
- certain adjustments, such as the deletion of the requirement that the encryption key must be in Luxembourg;
- the obligation to base an outsourcing (involving the disclosure of confidential data) on client consent is removed : indeed, this obligation shall be introduced in the Financial Sector Act 1993 as a legal exception to the professional secrecy obligation (the so-called banking secrecy) for outsourcing operations in the near future, so that there is no need to repeat this obligation in a circular (it being understood that the financial institution should nevertheless check whether it needs to inform its clients or whether it needs their consent under the Financial Sector Act 1993); and
- certain additions, such as the introduction of the principle that access to confidential data must take place in accordance with the principles of «need to know» and «least privilege».

Furthermore, **Circular CSSF 17/656** contains specific rules for activities that authorised support financial service providers within the meaning of Articles 29-1 to 29-6 of the Financial Sector Act 1993 (amongst which the authorised IT system operators) outsource themselves to another entity. The circular governs the following outsourcing situations:
- the use of infrastructures belonging to the group;
- the outsourcing of IT for internal purposes to a third party service provider; and
- the outsourcing by branches abroad to local service providers.

These support financial service providers must obtain the prior approval of their clients (i.e., regulated entities) if the outsourcing concerns information falling within the ambit of the clients' professional secrecy obligation.

2. Circular CSSF 17/654 on the use of cloud services («Cloud Circular»)

1. The CSSF has adopted a Cloud Circular specifically dealing with the use of cloud services by financial institutions. Cloud Circular is applicable to every outsourcing scheme that meets the traditional definition of cloud computing set forth by the NIST (on-demand self-service, broad network access, resource pooling, rapid elasticity and measured service) and on condition that:
- employees of the cloud computing service provider cannot have access to data and systems held by the financial institution in the cloud (i) without the prior and express authorisation of the financial institution and (ii) without the existence of a monitoring system of such access made available to the financial institution (such access must remain exceptional);
- the cloud computing services do not involve the manual interaction of the cloud service provider in the daily management of the cloud computing resources used by the financial institution.
The extent that the Cloud Circular is applicable, the outsourcing provisions in Circular CSSF 17/655 and Circular CSSF 17/656 shall not apply.

2. The Cloud Circular contains, in a nutshell, the following obligations (please note that this list is not exhaustive):

- if the operation of cloud resources (i.e., the management of cloud resources via the client's interface) is not in the hands of the client itself or has not been entrusted to an IT systems operator of the financial sector within the meaning of Articles 29-3 and 29-4 of the Financial Sector Act 1993, the client must proceed with a **detailed risk analysis** on the activities of the cloud service provider and in particular on the R&R matrix between the operator and the cloud service provider, the management of client segregation, audit rights on the part of the outsourcing entity, etc.

- the Cloud Circular contains several provisions on the **governance** of cloud services, including:
  - the appointment of a cloud officer for the cloud resources operating entity (client or third party service provider);
  - the need for an IT policy between a client and an operator (if the latter is an external provider);
  - the requirement that the outsourcing must be in line with a written outsourcing policy that has been approved by the authorised management (including an emergency and exit strategy);
  - the need for a written and documented R&R matrix and communication means, together with an obligation of information for the cloud service provider regarding any important problem impacting the outsourced activities; and
  - the client must understand and the operator (either the client or an external provider) must be able to control the risks related to cloud computing, such as the lack of segregation on a multi-tenant infrastructure, the laws and regulations of the countries where data is stored, the impact of the failure of a telecom network or service, the use of the cloud as a shadow IT system or the lack of system/ data portability.

- the regulated entity must assess whether its **clients must be informed or give its approval**;

- depending on the materiality of the activity supported by the cloud infrastructure, the regulated entity needs to obtain a **prior approval** from the CSSF; if such activities are not material or if the cloud service contract is signed with an IT systems operator of the financial sector within the meaning of Articles 29-3 and 29-4 of the Financial Sector Act 1993, a simple **notification** to the CSSF is sufficient;

- management of the risk related to a cloud based outsourcing:
  - there must be the expertise within the entity (client or external service provider) with respect to this type of outsourcing that is sufficient to effectively control the outsourced activities and manage the associated risks, and there must be sufficient internal knowledge about the impact of the use of SaaS programme;
  - the need for a prior and detailed analysis on (i) whether the outsourcing is in line with the principle of central administration, as well as on (ii) the risks of hosting of systems and data abroad, (iii) the criticality of the supported activities, (iv) any vendor lock-in effect, and (v) the risks related to chains of cloud based outsourcing;
  - coherence between the information system security policies of the client (i.e. regulated entity), the operator (if different) and the cloud service provider; and
  - changes in functionalities must be notified to the signatory of the cloud services contract prior to their implementation (the signatory can either be the operator or the client).

- continuity of services:
  - the client must be able to continue its critical activities in the event of exceptional circumstances or crises even when it is subject to a winding-up or liquidation procedure;
  - the client and the signatory of the cloud services contract must ensure that the transfer of the cloud based outsourced services can be insourced or transferred to another operator, each time that the continuity or the quality of the services risks to be compromised.

- system security:
  - the confidentiality and integrity of the data and systems must be guaranteed throughout the whole IT outsourcing chain, whereby access to data and systems must take place in accordance with the principles of «need to know» and «least privilege»;
  - IT links must allow for a rapid and unlimited access to stored information; and
  - the operator must obtain information about the security measures put in place by the cloud services provider and ensure that their configuration is in line with the client's security policy.

- contract clauses:
  - the law applicable to the cloud services contract must be the law of one of the EU Member States (exemptions can be requested to the CSSF for SaaS services);
  - a resilience of data and systems within the EU must be contractually foreseen (exemptions can be requested to the CSSF for SaaS services);
  - a contract must be in place between the client and the operator (if applicable);
  - qualitative and quantitative service levels must be provided;
  - upon the termination of the cloud services contract, the cloud service provider must delete the data and systems within a reasonable timeframe; and
  - audit rights for the CSSF and the signatory of the cloud services contract.

- control of activities:
  - via KPI measuring;
  - the segregation of client data and systems must be controlled, also with respect to multi-tenant infrastructures;
  - the internal control function of the client must have access to the data and systems hosted on the cloud infrastructure.

- audit rights:
  - via access to and review of audit and certification reports, if needed inclusion of non-covered elements to be foreseen contractually; and
  - (collective or individual) audit of processes, systems, premises, data and infrastructure to the extent that these would not be covered in the audit and/or certification reports.

3. Circular CSSF 17/657 updates Circular CSSF 06/240 on administrative and accounting organisation in order to carve out cloud services from the concept of «operation of IT systems», if offered by a Luxembourg entity to financial services providers, require a specific authorisation under the Financial Sector Act 1993. The question could be raised as to whether such exemption should not be laid down in the Financial Sector Act 1993 given that an exemption to a provision of the latter can only be adopted by law and not via CSSF circulars.

Concluding remarks

The new regulatory framework of the CSSF on the outsourcing accommodates the high demand of financial institutions to outsource activities, especially in the field of IT, offering more possibilities to do so and to use standard cloud services. However, where outsourcing is possible, it remains subject to rather strict conditions and to the control of the CSSF. In addition, some regulatory questions remain, such as the relationship between these new circulars and some other existing circulars in particular Circular CSSF 13/554 on the use and control of IT resources and the management of access to these resources. Indeed, when a multinational financial group including a Luxembourg entity wishes to use a general access tool for IT resources at the group level, Circular CSSF 13/554 requires the Luxembourg financial institution to introduce a formal, detailed authorisation request to the CSSF, proving it still has full control over the IT resources for which it is responsible. This circular will need to be complied with, in addition to the circulars on outsourcing of 17 May 2017.

Vincent WELLENS (cf. portrait), Avocat à la Cour
Partner NautaDutilh Avocats Luxembourg S.à r.l.
vincent.wellens@nautadutilh.com

Barbara GIROUD, Avocat au barreau de Paris
Inscrit au barreau de Luxembourg (Liste IV)
Associate NautaDutilh Avocats Luxembourg S.à r.l.
barbara.giroud@nautadutilh.com

Jad NADER ,
Counsel NautaDutilh Avocats Luxembourg S.à r.l.
jad.nader@nautadutilh.com

Les Luxembourgeois prêts à être assistés par un « robo-adviser »

Selon la dernière étude d'ING International Survey (IIS) sur le mobile banking, 44% des résidents luxembourgeois interrogés se sentent prêts à être assistés d'une façon ou d'une autre par un «robo-adviser». De quoi s'agit-il ? Un robo-adviser est un programme informatique qui enregistre les préférences du client et investit son argent pour lui dans les investissements qu'il pense être les plus adaptés à sa situation particulière.

Si l'on rentre dans le détail de ces 44%, on constate que 30% des résidents (contre 29% à l'échelle européenne) sont prêts à recevoir simplement les conseils, 12% (contre 26% à l'échelle européenne) sont prêts à accepter les décisions d'un robo-adviser mais moyennant validation finale par eux et 2% (contre 3% à l'échelle européenne) acceptent de laisser le contrôle total de leurs activités financières à un robo-adviser. Sur cette question, on constate davantage de réticence du côté des résidents nationaux, qui sont 56% à ne pas vouloir de service financier automatique, contre 48% pour les non-nationaux.

Quant à savoir si les résidents luxembourgeois accepteraient de voir leur application bancaire transférer automatiquement de l'argent de leur compte d'épargne vers leur compte courant lorsqu'ils sont à découvert, 30% ont répondu «oui», contre 34% à l'échelle européenne, 41% en France, 31% en Belgique et 26% en Allemagne.

Plus de détails sur www.mymoney.lu et www.ezonomics.com!