Commission de Surveillance du Secteur Financier

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

Luxembourg, 17 May 2017

To all credit institutions, investment firms and professionals performing lending operations

CIRCULAR CSSF 17/655

Re: **Update of Circular CSSF 12/552 on the central administration, internal governance and risk management**

Ladies and Gentlemen,

1. The purpose of this circular is to update Circular CSSF 12/552 on the central administration, internal governance and risk management. Circular CSSF 12/552 is amended as follows:

- In footnote no 3 on page 2, the first sentence "Circulars IML 95/120, IML 96/126, IML 98/143 and CSSF 05/178 shall remain applicable for PFS other than investment firms." is replaced by "Circulars IML 95/120, IML 96/126, IML 98/143 shall remain applicable for PFS other than investment firms, as well as Circular CSSF 17/656 which repeals and replaces Circular CSSF 05/178."
- In the 6th indent of point 17, after "the guiding principles as regards outsourcing", the following words are inserted: "including IT-related outsourcing relying on a cloud computing infrastructure or not".
- The following new paragraph is inserted after the third paragraph of point 85:

  "The institutions shall have a monitoring process in place in order to be quickly informed of the emergence of new security vulnerabilities, as well as a procedure to manage patches allowing the correction of these vulnerabilities, within a short period of time, if they can significantly impact their IT systems. Internal audit shall include the review of the monitoring process and the management of patches in its multi-annual audit plan; it shall notably state any failures in the launch of production of a patch while this patch is widely known and shall document such failure in an audit finding."
- The following new paragraph is inserted after the first paragraph of point 181:

  "Whereas IT outsourcing, or a chain of outsourcing exclusively composed of IT outsourcing, relies on a cloud computing infrastructure as defined in Circular CSSF

17/654, the points of sub-chapter 7.4 of this circular shall not apply and the financial professional shall comply with the requirements of Circular CSSF 17/654."

- The second paragraph of point 182 is amended as follows:
  - The 6th indent:

    "The institution shall assess, in view of possible legal or other risks, whether or not the third parties concerned by this outsourcing, in particular customers, should be informed;"

    is replaced by:

    "The institution shall assess, in view of possible legal risks and legal obligations, whether or not the third parties concerned by this outsourcing, and in particular financial sector customers, should be informed, or their consent be obtained. In this respect, the institution shall comply with the regulations in force relating to personal data protection."

  - The 7th indent:

    "Data confidentiality shall be guaranteed at all times, unless explicit consent is given by the customer or the owner of the data or his/her proxy, on the basis of an informed opinion on the purpose of this outsourcing, specific nature of the final goal, the content of the provided information, the recipient and location as well as of the sustainability;"

    is replaced by:

    "The confidentiality and integrity of data and systems shall be controlled throughout the outsourcing chain. In particular, access to data and systems shall fulfil the principles of "need to know" and "least privilege", i.e. access is only granted to persons whose functions so require, for a specific purpose, and their privileges shall be limited to the strict necessary minimum to exercise their functions;"

  - At the end of the 8th indent, the reference to the articles of the PFS is extended as follows: "according to Articles 29-1 to 29-6 of the LFS".

- At point 188:
  - The second sentence:

    "The institution shall be able to continue to operate normally in case of exceptional events or crisis."

    is replaced by:

    "The institution shall be able to continue its critical functions in case of exceptional events or crisis."

  - The third sentence:

    "In this respect, the outsourcing agreements shall not include termination clauses or service termination clauses because of reorganisation measures or a winding-up procedure applied to the institution, as provided for in Part IV of the LFS."

    is replaced by:

    "In this respect, the outsourcing agreements shall not include termination clauses or service termination clauses because of resolution actions or reorganisation measures

or a winding-up procedure applied to the institution, as provided for in the Law of 18 December 2015 on the failure of credit institutions and certain investment firms."

- In the first sentence of point 190, "and its subcontractor(s)" is replaced by "and all the actors in the outsourcing chain."

- At point 193:

  - Under the indent "In Luxembourg, solely from:", the second sub-indent:

  "an entity of the group to which the institution belongs and which exclusively deals with group transactions provided that these systems do not include any readable confidential data on the customers other than institutional customers, unless explicit consent is given by the customer or the owner of the data or his/her proxy, on the basis of an informed opinion on the purpose of this outsourcing, the specific nature of the final goal, of the content of the provided information, of the recipient and location as well as of the sustainability; in respect of institutional customers, the specific characteristics of this outsourcing shall be made explicit in the agreement."

  is replaced by:

  "an entity of the group to which the institution belongs and which exclusively deals with group transactions, provided that these systems do not include any readable confidential data on the customers. Otherwise, the institution shall assess, in view of possible legal risks and legal obligations, whether or not the third parties concerned by this outsourcing, and in particular financial sector customers, should be informed, or their consent be obtained. In this respect, the institution shall comply with the regulations in force relating to personal data protection."

  - Under the indent "Abroad, from:" the sub-indent:

  "an entity of the group to which the institution belongs provided that these systems do not include any readable confidential data on customers other than institutional customers, unless explicit consent is given by the customer or the owner of the data or his/her proxy, on the basis of an informed opinion on the purpose of this outsourcing, the specific nature of the final goal, of the content of the provided information, of the recipient and location as well as of the sustainability; in respect of institutional customers, the specific characteristics of this outsourcing shall be made explicit in the agreement."

  is replaced by:

  "any IT service provider, including an entity of the group to which the institution belongs, provided that these systems do not include any readable confidential data on customers. Otherwise, the institution shall assess, in view of possible legal risks and legal obligations, whether or not the third parties concerned by this outsourcing, and in particular financial sector customers, should be informed, or their consent be obtained. In this respect, the institution shall comply with the regulations in force relating to personal data protection."

- The first two sentences of point 195:

  "Prohibition to access confidential data shall also be applicable to third-party subcontractors other than support PFS which provide consulting, development or

maintenance services. These third parties shall operate by default outside the IT production system."

are replaced by:

"Third-party subcontractors other than support PFS which provide consulting, development or maintenance services shall operate by default outside the IT production system."

- The second paragraph of point 198:
  - In the first sentence, "or of the Luxembourg credit institution" is inserted after "only the staff of the support PFS".
  - The last sentence:

"Where the subcontractor is not a support PFS, it cannot intervene on the premises of the institution without being accompanied, throughout its mission, by a person of the institution in charge of IT."

is replaced by:

"Where the subcontractor is not a support PFS or a Luxembourg credit institution, the institution shall assess, in view of possible legal risks and legal obligations, whether or not the third parties concerned by this outsourcing, and in particular financial sector customers, should be informed, or their consent be obtained. Otherwise, the subcontractor cannot intervene on the premises of the institution without being accompanied, throughout its mission, by a person of the institution in charge of IT."

- Point 201:

"Where the processing centre is abroad, no confidential data which enables the identification of a customer of the institution can be stored therein, unless it is encrypted and provided that the decryption can only be carried out within the institution or a support PFS within the context of its service provision or if all customers of the institution fulfil the conditions of express and informed consent as defined in point 193."

is replaced by:

"Where the processing centre is abroad, no confidential data which enables the identification of a customer of the institution can be stored therein, unless it is protected. The confidentiality and integrity of data and systems shall be controlled throughout the IT outsourcing chain. In particular, access to data and systems shall fulfil the principles of "need to know" and "least privilege", i.e. access is only granted to persons whose functions so require, with a specific purpose, and their privileges shall be limited to the strict necessary minimum to exercise their functions. The institution shall assess, in view of possible legal risks and legal obligations, whether or not the third parties concerned by this outsourcing, and in particular financial sector customers, should be informed, or their consent be obtained."

Entry into force and other provisions

2. The changes brought by this circular to Circular CSSF 12/552 shall enter into force with immediate effect.

Yours faithfully,

COMMISSION de SURVEILLANCE du SECTEUR FINANCIER

Jean-Pierre FABER
Director

Françoise KAUTHEN
Director

Claude SIMON
Director

Simone DELCOURT
Director

Claude MARX
Director General