Art. 1. Customer due diligence

(1) The obligation to identify the customer and to verify the customer's identity as provided in Article 3(2)(a) of the amended law of 12 November 2004 on the fight against money laundering and terrorist financing (the “Law”) shall also include, if applicable, the identification of the proxies as well as the verification of their identity and of their power to act on behalf of the client.

In particular for customers that are legal persons or legal arrangements, the obligation to identify the customer and to verify the customer's identity includes the obligation to:

(a) verify that any person purporting to act on behalf of the customer is so authorised, and identify and verify the identity of that person; and

(b) verify the legal status of the legal person or legal arrangement, e.g. by obtaining proof of incorporation or similar evidence of establishment or existence, and obtain information concerning the customer's name, the names of trustees (for trusts), legal form, address, directors (for legal persons), and provisions regulating the power to bind the legal person or arrangement.

(2) The obligation to identify the beneficial owner and to verify the beneficial owner's identity as provided in Article 3(2)(b) of the Law, shall also include the obligation to take reasonable measures to verify the beneficial owner's identity using relevant information or data obtained from a reliable source such that the professional is satisfied that it knows who the beneficial owner is.

For all customers, the obligation to identify the beneficial owner requires determining whether the customer is acting on behalf of another person and to take then reasonable steps to obtain sufficient identification data to verify that other person's identity.
For customers that are legal persons or legal arrangements, the obligation to identify the beneficial owner requires that reasonable measures be taken to:

(a) understand the ownership and control structure of the customer;
(b) determine who are the natural persons that ultimately own or control the customer. This includes those persons who exercise ultimate effective control over a legal person or arrangement.

The types of measures that would be normally needed to satisfactorily perform this function shall include amongst others:

– for companies: identifying the natural persons with a controlling interest and the natural persons who comprise the mind and management of company;
– for trusts: identifying the settlor, the trustee or person exercising effective control over the trust, and the beneficiaries.

(3) The obligation to carry out an ongoing due diligence of the business relationship shall include scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the institution's knowledge of the customer, their business and risk profile, and where necessary, the source of funds.

Professionals shall ensure that documents, data or information collected under the customer due diligence process is kept up-to-date and relevant by undertaking reviews of existing records, particularly for higher risk categories of customers or business relationships.

The obligation to carry out an ongoing due diligence of the business relationship shall also include the obligation to pay special attention to all complex, unusual large transactions, or unusual patterns of transactions, that have no apparent economic or lawful purpose.

Special attention shall notably be paid to: significant transactions relative to a business relationship, transactions that exceed certain limits, very high account turnover inconsistent with the size of the balance, or transactions which fall out of the regular pattern of the account's activity.

Professionals shall scrutinise as far as possible the background and purpose of such transactions, set forth their findings in writing and keep these documents in accordance with Article 3(6)(b) of the Law and to keep them available for the competent authorities and auditors for at least five years, without prejudice to longer record-keeping periods prescribed by other laws.

(4) In order to apply due diligence measures to existing customers, "appropriate times on a risk-sensitive basis" within the meaning of Article 3(5) of the Law is, either
where the risk is high, or where a numbered account exists, or where a situation occurs justifying these measures and particularly in the following situations:

- where a transaction of significance takes place;
- where customer documentation standards change substantially;
- as regards banking business, where there is a material change in the way that a customer's account is operated;
- where the professional becomes aware that it lacks sufficient information about an existing customer.

(5) The record-keeping obligation of documents and information as provided in Article 3(6) of the Law shall include the obligation to maintain records of the identification data, account files and of the business correspondence for at least five years following the termination of an account or business relationship, without prejudice to any longer record-keeping periods prescribed by other laws. If a competent authority requests, in specific cases and for the fulfilment of its mandate, to apply a longer record-keeping period than the minimum period provided above, the professional shall comply with this request.

Transaction records shall be sufficient to permit reconstruction of individual transactions so as to provide, if necessary, evidence for prosecution of criminal activity.

Together, the different components of transaction records shall thus provide, in particular, the following information: customer's and beneficiary's name, address or other identifying information normally recorded by the intermediary, the nature and date of the transaction, the type and amount of currency involved, and the type and identifying number of any account involved in the transaction.

Professionals shall ensure that all the above-mentioned transaction records and information are available to the competent authorities, when acting in the context of their mandate, so that professionals may respond promptly to information requests by such authorities.

(6) Both customer due diligence in general and the assessment of the extent of measures to be applied on a risk-sensitive basis in particular, shall be consistent with the guidelines issued by the competent authorities, for instance in the form of circulars.

**Art. 2. Simplified customer due diligence**

It is not mandatory to apply the simplified customer due diligence regime as set out in Article 3-1 of the Law and is therefore not imposed on professionals.

The obligation to gather sufficient information in any circumstances so as to establish whether the customer meets the necessary conditions for Article 3-1 of the Law to apply, shall at least include customer identification and monitoring of the business relationship so that the necessary conditions for Article 3-1 of the Law are always met.
and the verification that there is no suspicion of money laundering or terrorist financing. This obligation also applies to the situations referred to in Article 3-1(4) of the Law.

(Grand-ducal Regulation of 5 August 2015)
“The professionals may reduce the identification measures and need not verify the identity of their customer and, where applicable, the beneficial owner of the business relationship when they carry out online payment services fulfilling each of the following conditions:

1. the transaction concerns the provision of payment services listed under number 3, second and third indents, number 4, second and third indent, number 5 and number 7 of the Annex to the law of 10 November 2009 on payment services, as amended;
2. the transaction is executed via accounts held with payment service providers located in the EU or in a third country which imposes equivalent requirements relating to the fight against money laundering and terrorist financing;
3. the transaction does not exceed a unit amount of EUR 250;
4. the total amount of the transactions executed for the customer during the 12 months preceding the transaction does not exceed EUR 2,500.

The possibility not to verify the identity of the customer and, where applicable, of the beneficial owner of the business relationship, also applies to professionals with respect to electronic money referred to in Article 3-1(4)(d) of the Law.”

The simplified customer due diligence regime is excluded when there is a suspicion of money laundering or terrorist financing, when there are doubts about the veracity or adequacy of previously obtained data or in specific circumstances which carry a higher risk.

Art. 3. Enhanced customer due diligence

(1) Business relationships and transactions including with natural persons, legal persons or financial institutions from or in a country which does not apply or insufficiently applies the measures for the fight against money laundering and terrorist financing are situations carrying a higher risk within the meaning of Article 3-2(1) of the Law, requiring special attention and enhanced customer due diligence. Where those transactions have no apparent economic or visible lawful purpose, the background and purpose of such transactions shall, as far as possible, be scrutinised, the findings shall be set forth in writing in order to be available to auditors and competent authorities in accordance with the latter's instructions.

Supervisors and, where applicable, self-regulatory bodies of the different professionals shall inform the professionals of concerns about country-specific loopholes
in the relevant provisions for the fight against money laundering and terrorist financing of the countries referred to above.

Where a country continues not to apply or insufficiently applies measures for the fight against money laundering and terrorist financing, these authorities and bodies shall warn the professionals about the risks of money laundering and terrorist financing in transactions with natural or legal persons of that country. They may set out specific measures based on a case-by-case approach which professionals must implement upon having noticed a risk.

Examples of such specific measures include, but are not restricted to:

- stringent requirements for identifying clients and enhancement of advisories, including jurisdiction-specific financial advisories, to financial institutions for identification of the beneficial owners before business relationships are established with individuals or companies from these countries;
- enhanced relevant reporting mechanisms or systematic reporting of financial transactions on the basis that financial transactions with such countries are more likely to be suspicious.

(2) For non-face-to-face transactions, the professionals shall have policies and procedures in place to address any specific risks associated with such business relationships or transactions. These policies and procedures shall apply when establishing customer relationships and when conducting ongoing due diligence.

Non-face-to-face operations include business relationships concluded over the Internet or by other means such as through the post, services and transactions over the Internet including trading in securities by retail investors over the Internet or other interactive computer services, use of ATM machines, telephone banking, transmission of instructions or applications via facsimile or similar means and making payments and receiving cash withdrawals as part of electronic point of sale transaction using prepaid or reloadable or account-linked value cards.

Measures for managing the risks shall include specific and effective customer due diligence procedures that apply to non-face-to-face customers. Such procedures include e.g. the certification of documents presented, the requisition of additional documents to complement those which are required for face-to-face customers, developing independent contact with the customer, the use of third party introduction or the requirement of the first payment to be carried out through an account in the customer's name with another credit institution subject to similar customer due diligence standards.

(3) In relation to cross-border correspondent banking relationships referred to in Article 3-2(3) of the Law, credit institutions shall also:

- determine from publicly available information the reputation of the respondent institution and the quality of its supervision, including whether the institution
concerned has been subject to a money laundering or terrorist financing investigation or regulatory action;

- assess the respondent institution's controls against money laundering and terrorist financing and ascertain that they are adequate and effective;
- document the respective responsibilities in the fight against money laundering and terrorist financing of each institution.

The authorisation procedure which requires approval from the senior management includes the authorisation by the senior management and involves the anti-money laundering and terrorist financing compliance officer.

Where a correspondent banking relationship involves the maintenance of "payable-through" accounts, credit institutions shall be satisfied that:

(a) their customer (the respondent credit institution) has performed all the normal customer due diligence obligations set out in Article 3 of the Law on those of its customers that have direct access to the accounts of the correspondent institution; and

(b) the respondent credit institution is able to provide relevant customer identification data upon request to the correspondent institution. A Luxembourg credit institution is authorised to provide such information within the framework of a correspondent banking relationship.

To the extent other institutions which are not credit institutions are involved in correspondent banking relationships, these rules shall equally apply to these institutions.

(4) Enhanced customer due diligence for politically exposed persons shall also apply when this person carries out a prominent public function in another Member State or in a third country or on behalf of the Member State or the third country.

Professionals shall put in place appropriate risk management systems to determine whether a potential customer, a customer or the beneficial owner is a politically exposed person.

Where a customer has been accepted and the customer or beneficial owner is subsequently found to be, or subsequently becomes a politically exposed person, professionals shall obtain approval to continue the business relationship from the senior management.

The authorisation procedure requiring approval from the senior management shall include the authorisation by senior management and involves the anti-money laundering and terrorist financing compliance officer.

Professionals shall take reasonable measures to establish the source of wealth and the source of funds of customers and beneficial owners identified as politically exposed persons.
Where professionals are in a business relationship with a politically exposed person, they shall be required to conduct enhanced ongoing monitoring on that relationship.

**Art. 4. Obligations of branches and subsidiaries in foreign countries**

The customer due diligence requirements laid down in Article 2(2) of the Law with which the branches and subsidiaries in third countries shall comply include all of the requirements listed in Article 3 of the Law and particularly those set out in paragraph 2 of this article.

Credit institutions and financial institutions shall pay particular attention that this principle is observed with respect to their branches and subsidiaries in countries which do not or insufficiently apply the requirements regarding the fight against money laundering and terrorist financing.

Where the minimum requirements for the fight against money laundering and terrorist financing of host countries differ from those applicable in Luxembourg, branches and subsidiaries in host countries shall apply the higher standard, to the extent that host country laws and regulations permit.

**Art. 5. Prohibition of accounts and passbooks in fictitious names**

Customer due diligence procedures and requirements for the recording and the keeping of documents prohibit that accounts and passbooks be kept in fictitious names.

However, credit institutions and financial institutions are authorised to keep numbered accounts provided such institutions strictly comply with the specific set of rules drawn up by them to that effect. These rules shall lay down the account opening conditions and shall specify how they operate. These rules shall ensure that these accounts are managed so as to fully comply with the provisions of the Law, in particular with the provisions on customer due diligence procedures, the recording and keeping of data and the unrestricted access to these data both for compliance officers responsible for the fight against money laundering and terrorist financing and for other appropriate staff, as well as for competent authorities.

**Art. 6. Performance of customer due diligence by third parties**

(1) Professionals relying upon a third party under Article 3-3 of the Law shall immediately obtain from the third party the necessary information concerning the following elements of the customer due diligence process:

- identification of customers and, if appropriate, of their proxies;
- identification of the beneficial owners;
- purpose and intended nature of the business relationship.
(2) Professionals shall take adequate steps to satisfy themselves that copies of identification data and other relevant documentation relating to customer due diligence requirements will be made available from the third party upon request without delay.

(3) Professionals shall also satisfy themselves that the third party is regulated and supervised, and that it has implemented measures to comply with customer due diligence requirements. A third party may not, under any circumstances, be established in a country which does not apply or insufficiently applies the measures for the fight against money laundering and terrorist financing.

**Art. 7. Appropriate internal management requirements**

(1) Appropriate internal management requirements shall include the obligation to establish and maintain internal procedures, policies and controls to prevent money laundering and terrorist financing and communicate these to employees. These procedures, policies and controls shall cover, *inter alia*, customer due diligence, record-keeping, the detection of unusual or suspicious transactions and the obligation to report suspicious transactions.

(2) An appropriate internal management shall include the development of appropriate compliance management arrangements, e.g. the appointment of at least one anti-money laundering and terrorist financing compliance officer at the management level. The internal control arrangements, including the audit function, shall be adequately resourced to test compliance, including sample testing, with these procedures, policies and controls and they shall enjoy the independence which is necessary to perform their tasks.

The anti-money laundering and terrorist financing compliance officer and other appropriate staff members shall have timely access to customer identification data and other customer due diligence information, transaction records, and other relevant information. The anti-money laundering and terrorist financing compliance officer shall be able to act independently and to report directly to senior management, without having to report to the next reporting level or to the board of directors.

(3) An appropriate internal management shall also include the putting into place of ongoing employee training to ensure that employees are kept informed of new developments, including information on current money laundering and terrorist financing techniques, methods and trends and that they receive a clear explanation of all aspects of legal obligations relating to the fight against money laundering and terrorist financing, and in particular requirements concerning customer due diligence and suspicious transaction reporting.

(4) An appropriate internal management shall also include the putting into place of appropriate screening procedures to ensure high standards when hiring employees.
An appropriate internal management shall also include the putting into place of the necessary measures to prevent the misuse of technological developments for money laundering or terrorist financing.

Art. 8. Cooperation requirements with the authorities

(1) The obligation to communicate information referred to in Article 5(1)(b) of the Law shall include the communication of existing documents on which this information is based.

(2) Pursuant to Article 5(1)(a) of the Law, the obligation to report suspicious transactions shall apply for each fact which might be an indication of money laundering or terrorist financing due, in particular for reasons relating to the person concerned, to his development, to the source of the funds, to the nature, the purpose or procedures of the transactions, without the reporting person classifying the underlying offence.

Particularly in the fight against terrorist financing, this reporting obligation shall also apply to funds for which there are reasonable grounds to suspect or they are suspected to be linked or related to, or to be used for terrorism, terrorist acts or by terrorist associations, organisations or groups or by those who finance terrorism, without limiting this obligation solely to funds of persons listed by the United Nations or by the European Union in the context of the fight against terrorism.

(3) An information request relating to the fight against money laundering and terrorist financing pursuant to Article 5(1)(b) of the Law or an instruction to freeze pursuant to paragraph 3 of this article does not presuppose a prior information according to paragraph (1)(a) of this article but these measures may also be taken by the State prosecutor in his capacity as financial intelligence unit, in the absence of a suspicious transaction report from a professional.

For the purposes of executing Article 5(1)(b) of the Law, the State prosecutor referring to a money laundering or terrorist financing investigation shall communicate either a written or an oral request based on this article. Where the request is communicated orally, it must be followed by a written confirmation within 3 days.

A freezing instruction pursuant to Article 5(3) of the Law may be sent simultaneously via a circular to several professionals and may refer to the funds of one or more persons at the same time.

(4) The adequate and appropriate procedure regarding the communication referred to in Article 4(1) of the Law shall include procedures enabling professionals to respond rapidly and fully to any information request from the Luxembourg authorities in charge of the fight against money laundering and terrorist financing.
(5) The protection for disclosures made in good faith under Article 5(4) of the Law shall apply even if the reporting person was not fully aware what the actual illegal activity was and regardless of whether illegal activity actually occurred.

Art. 9. Sanctions

Any person breaching the professional obligations as specified in this grand-ducal regulation shall incur a fine or sanctions in accordance with Article 9 of the Law.

Art. 10. Our Minister of Finance shall execute this regulation, which shall be published in the Mémorial.